

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

_____)	
SECURITIES AND EXCHANGE COMMISSION,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 23-cv-9518-PAE
)	
SOLARWINDS CORP. and TIMOTHY G.)	
BROWN,)	
)	
Defendants.)	
_____)	

**PLAINTIFF SECURITIES AND EXCHANGE COMMISSION’S
OPPOSITION TO DEFENDANTS’ MOTION TO DISMISS**

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
SUMMARY OF ALLEGATIONS	3
A. General Background	3
B. SolarWinds and Brown Made Misleading Public Statements Regarding SolarWinds’ Cybersecurity Practices.....	4
1. Brown Drives SolarWinds to Post the False Security Statement.....	4
2. SolarWinds Made False Risk Disclosures in Its SEC Filings.....	5
C. SolarWinds and Brown Failed to Disclose Red Flags and Warning Signs of a Cyberattack Leading up to the Revelation of the SUNBURST Cyberattack	5
1. Defendants Failed to Adequately Respond to Warnings of a Security Gap.....	5
2. The Defendants Did Not Address Increasing Attacks.....	6
D. Once SolarWinds Learned of the SUNBURST Attack, It Did Not Fully Disclose Its Known Impact.....	7
ARGUMENT	8
I. Standard of Review.....	8
II. The Amended Complaint Sufficiently Alleges Fraud.....	8
A. The Legal Standards Applicable to Securities Fraud Claims.....	8
B. The Amended Complaint Sufficiently Alleges Misstatement Liability Under Rule 10b-5(b) and Section 17(a)(2).....	10
1. The Security Statement’s Representations Were False and Misleading	10
a. SolarWinds Misleadingly Claimed to “Follow” the NIST Cybersecurity Framework	11
b. SolarWinds Evaluated Its Cybersecurity Using the NIST 800-53 But Failed to Disclose the Problems It Found	13
c. SolarWinds Had “Significant Deficiencies” in Its Access Controls.	14

d. SolarWinds’ Own Documents Show It Did Not Follow a Secure Development Lifecycle.	16
e. SolarWinds’ Own Documents Show Pervasive Network Monitoring Failures. .	17
f. SolarWinds Had Pervasive Password Policy Violations	18
g. SolarWinds’ Cybersecurity Problems Were Systemic	18
2. The False Statements in the Security Statement Were Material	19
3. Brown’s Other Public Statements Were Materially False and Misleading	22
4. SolarWinds’ Generic Risk Disclosures in Its SEC Filings Were False and Misleading.....	23
a. Companies Cannot Rely on Generic Disclosures	23
b. SolarWinds’ Generic Disclosure that It Was “Vulnerable” to Cybersecurity Threats Failed to Provide Investors With Material Information About SolarWinds’ Specific Risk Profile	25
c. The Cases Relied Upon by SolarWinds Did Not Involve Omission of Specific Material Risks	27
d. SolarWinds Presents a False Dichotomy Between Its Generic, Boilerplate Risk Disclosures and “Granular” Disclosures that Would Provide a “Roadmap” to Threat Actors.....	29
5. The Information Omitted from the Risk Disclosures Was Material	32
6. SolarWinds’ Incomplete SUNBURST Disclosure in Its December 14, 2020 8-K Was Materially False and Misleading	34
C. The Amended Complaint Sufficiently Alleges Scheme Liability	36
D. The Amended Complaint Sufficiently Alleges Scienter	38
1. Legal Standard for Scienter	38
2. Brown Knew the Security Statement Was False.....	39
3. Brown Knowingly Provided False Information Related to the Risk Disclosures ...	40
4. Brown Was Tasked with Ensuring the December Form 8-K Was Technically Accurate, and Knew It Was Not.....	41

5. Scienter for Scheme Liability Is Supported by Knowing or Reckless Dissemination of False Statements and Other Acts	42
III. The Amended Complaint Sufficiently Alleges Internal Accounting Controls Violations	43
A. Internal Accounting Controls Are Broader Than Controls Relating to Financial Reporting.....	44
B. Case Law Supports that Internal Controls Are Not Limited to Controls Related to Financial Statements	46
C. The ICFR Provision of the Sarbanes-Oxley Act Is Not Synonymous with the Internal Accounting Controls of the FCPA	48
D. SolarWinds’ Products, Source Code, IT Infrastructure and Customer Databases Are Precisely the Types of “Assets” that SolarWinds’ Management Should Have Safeguarded.....	49
IV. The Amended Complaint Sufficiently Alleges Disclosure Controls Violations	50
A. Public Companies Must Maintain Effective Disclosure Controls	50
B. The Failure to Escalate Critical Information Shows that SolarWinds’ Controls Were Not Effectively Maintained.....	51
C. Defendants’ View of Disclosure Controls Is Too Narrow	52
D. Misstatements About Controls Are Not the Same Thing as Failing to Maintain Effective Controls	53
V. The Amended Complaint Sufficiently Alleges Aiding and Abetting Liability	53
VI. Amici’s Policy Arguments Do Not Detract from the Sufficiency of the Allegations in the Amended Complaint	55
A. The Securities Laws Do Not Require Perfect Cybersecurity, but They Do Require Accurate Disclosures.....	57
B. The Securities Laws Do Not Require Roadmaps, but They Do Require Accurate Disclosures	58
C. Required Disclosures Should Not Undermine Open Communication or Internal Assessments	58
CONCLUSION	60

TABLE OF AUTHORITIES

CASES

<i>Arora v. HDFC Bank Ltd.</i> , 671 F. Supp. 3d 305 (E.D.N.Y. 2023)	53
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	8, 11
<i>Basic Inc. v. Levinson</i> , 485 U.S. 224 (1988)	19, 32
<i>Beleson v. Schwartz</i> , 419 F. App'x 38 (2d Cir. 2011)	36
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	8
<i>Bricklayers & Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd.</i> , 866 F. Supp. 2d 223 (S.D.N.Y. 2012)	16, 41
<i>City of Austin Police Ret. System v. Kinross Gold Corp.</i> , 957 F. Supp. 2d 277 (S.D.N.Y. 2013)	31, 32, 33, 41
<i>ECA, Local 134 IBEW Joint Pension Tr. of Chicago v. JP Morgan Chase Co.</i> , 553 F.3d 187 (2d Cir. 2009)	22
<i>Freudenberg v. E*Trade Fin. Corp.</i> , 712 F. Supp. 2d 171 (S.D.N.Y. 2010)	32, 33
<i>Ganino v. Citizens Utils. Co.</i> , 228 F.3d 154 (2d Cir. 2000)	19, 36
<i>Garnett v. RLX Tech. Inc.</i> , 632 F. Supp. 3d 574 (S.D.N.Y. 2022)	28, 29
<i>Higginbotham v. Baxter Int'l, Inc.</i> , 495 F.3d 753 (7th Cir. 2007)	53
<i>Hill v. Gozani</i> , 638 F.3d 40 (1st Cir. 2011)	33
<i>Ikon Office Solutions, Inc. Sec. Litig.</i> , 277 F.3d 658 (3d Cir. 2002)	47
<i>In re Bank of Am. AIG Disclosure Sec. Litig.</i> , 980 F. Supp. 2d 564 (S.D.N.Y. 2013)	30
<i>In re BHP Billiton Ltd. Sec. Litig.</i> , 276 F. Supp. 3d 65 (S.D.N.Y. 2017)	23
<i>In re BP p.l.c. Sec. Litig.</i> , 843 F. Supp. 2d 712 (S.D. Tex. 2012)	28

<i>In re Carter-Wallace Inc. Sec. Litig.</i> , 150 F.3d 153 (2d. Cir. 1998)	11
<i>In re Carter-Wallace Inc. Sec. Litig.</i> , 220 F.3d 36 (2d Cir. 2000)	38
<i>In re Citigroup, Inc. Sec. Litig.</i> 330 F. Supp. 2d 367 (S.D.N.Y. 2004)	36
<i>In re Elan Corp. Sec. Litig.</i> , 543 F. Supp. 2d 187 (S.D.N.Y. 2008)	47
<i>In re Equifax Inc. Sec. Litig.</i> , 357 F. Supp. 3d 1189 (N.D. Ga. 2019)	passim
<i>In re Fannie Mae 2008 Sec. Litig.</i> , 742 F. Supp. 2d 382 (S.D.N.Y.2010)	27
<i>In re FBR Inc. Sec. Litig.</i> , 544 F. Supp. 2d 346 (S.D.N.Y. 2008)	28
<i>In re Heartland Payments Systems, Inc. Sec. Litig.</i> , No. 09-cv-1043,2009 WL 4798148 (D.N.J. 2009)	34
<i>In re Hebron Tech. Co., Ltd. Sec. Litig.</i> , No. 20-cv-4420 (PAE), 2021 WL 4341500 (S.D.N.Y. Sept. 22, 2021)	53
<i>In re Intel Corp. Sec. Litig.</i> , No. 18-cv-00507-YGR, 2019 WL 1427660 (N.D. Cal. 2019)	30, 33
<i>In re Marriott Int'l, Inc.</i> , 31 F.4th 898 (4th Cir. 2022)	33
<i>In re Morgan Stanley Info. Fund Sec. Litig.</i> , 592 F.3d 347 (2d Cir. 2010)	12, 30, 35
<i>In re N. Telecom Ltd. Sec. Litig.</i> , 116 F. Supp. 2d 446 (S.D.N.Y. 2000)	30
<i>In re ProShares Tr. Sec. Litig.</i> , 728 F.3d 96 (2d Cir. 2013)	32
<i>In re Prudential Sec. Inc. Ltd. P'ships Litig.</i> , 930 F. Supp. 68 (S.D.N.Y. 1996)	29
<i>In re Qudian Sec. Litig.</i> , No. 17-cv-9741(JMF), 2019 WL 4735376 (S.D.N.Y. Sept. 27, 2019)	27
<i>In re Sanofi Sec. Litig.</i> , 87 F. Supp. 3d 510 (S.D.N.Y. 2015)	8, 28
<i>In re SolarWinds Corp. Sec. Litig.</i> , 595 F. Supp. 3d 573 (W.D. Tex. 2022)	passim

<i>In re ValuJet, Inc. Sec. Litig.</i> , 984 F. Supp. 1472 (N.D. Ga. 1997)	34
<i>In re Van der Moolen Holding N.V. Sec. Litig.</i> , 405 F. Supp. 2d 388 (S.D.N.Y. 2005)	27, 35
<i>In re Virtus Inv. Partners, Inc. Sec. Litig.</i> , 195 F. Supp. 3d 528 (S.D.N.Y. 2016)	22
<i>Kleinman v. Elan Corp. plc</i> , 706 F.3d 145 (2d Cir. 2013)	12
<i>Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC</i> , 797 F.3d 160 (2d Cir. 2015)	40
<i>Lorenzo v. SEC</i> , 587 U.S. 71 (2019)	37, 54
<i>Macquarie Infrastructure Corp. v. Moab Partners, L.P.</i> , No. 22-1165, 2024 WL 1588706 (U.S. Apr. 12, 2024)	12, 29
<i>Meyer v. Jinkosolar Holdings Co., Ltd.</i> , 761 F.3d 245 (2d Cir. 2014)	passim
<i>Novak v. Kasaks</i> , 216 F.3d 300 (2d Cir. 2000)	22, 38
<i>Ong v. Chipotle Mexican Grill, Inc.</i> , 294 F. Supp. 3d 199 (S.D.N.Y. 2018)	30
<i>Rex & Roberta Ling Living Trust v. B Commc'n Ltd.</i> , 346 F. Supp. 3d 389 (S.D.N.Y. 2018)	40, 42
<i>Richman v. Goldman Sachs Grp., Inc.</i> , 868 F. Supp. 2d 261 (S.D.N.Y. 2012)	23, 33
<i>S. Cherry St., LLC v. Hennessee Grp. LLC</i> , 573 F.3d 98 (2d Cir. 2009)	39, 42
<i>SEC v. Apuzzo</i> , 689 F.3d 204 (2d Cir. 2012)	54
<i>SEC v. AT&T, Inc.</i> , 626 F. Supp. 3d 703 (S.D.N.Y. 2022)	11
<i>SEC v. Cavco Indus. Inc., et al.</i> , No. 2:21-cv-01507, 2022 WL 1491279 (D. Ariz. Jan. 25, 2022)	46
<i>SEC v. China Ne. Petroleum Holdings Ltd.</i> , 27 F. Supp. 3d 379 (S.D.N.Y. 2014)	9
<i>SEC v. DCI Telecomms.</i> , 122 F. Supp. 2d 495 (S.D.N.Y. 2000)	11

<i>SEC v. DeFrancesco, No. 23-cv-131 (JSR),</i> 2023 WL 4631449 (S.D.N.Y. July 20, 2023)	25
<i>SEC v. DiMaria,</i> 207 F. Supp. 3d 343 (S.D.N.Y. 2016)	9
<i>SEC v. Enters. Solutions, Inc.,</i> 142 F. Supp. 2d 561 (S.D.N.Y. 2001)	11
<i>SEC v. Farnsworth,</i> No. 22-cv-8226, (KPF), 2023 WL 5977240 (S.D.N.Y. Sept. 14, 2023)	54
<i>SEC v. Felton,</i> No. 20-cv-822, (G), 2021 WL 2376722 (N.D. Tex. 2021)	47
<i>SEC v. First Jersey Sec., Inc.,</i> 101 F.3d 1450 (2d Cir. 1996)	9, 38
<i>SEC v. Gabelli,</i> 653 F.3d 49 (2d Cir. 2011)	12, 17
<i>SEC v. Ginder,</i> 752 F.3d 569 (2d Cir. 2014)	9
<i>SEC v. Koenig,</i> 469 F.2d 198 (2d Cir. 1972)	27
<i>SEC v. McNulty,</i> 137 F.3d 732 (2d Cir. 1998)	27
<i>SEC v. Monarch Funding Corp.,</i> 192 F.3d 295 (2d Cir. 1999)	9, 37
<i>SEC v. Patel,</i> No. 07-cv-39, (SM), 2009 WL 3151143 (D.N.H. Sept. 30, 2009)	47
<i>SEC v. Rio Tinto Ltd.,</i> No. 17-cv-7994 (AT), 2019 WL 1244933 (S.D.N.Y., Mar. 18, 2019)	47
<i>SEC v. Rio Tinto,</i> 41 F.4th 47 (2d. Cir. 2022)	37
<i>SEC v. Stoker,</i> 865 F. Supp. 2d 457 (S.D.N.Y. 2012)	39
<i>SEC v. Tolstedt,</i> 545 F. Supp. 3d 788 (N.D. Cal. 2021)	56
<i>SEC v. U.S. Env'tl., Inc.,</i> 155 F.3d 107 (2d. Cir. 1998)	38
<i>SEC v. Wilcox,</i> 663 F. Supp. 3d 146 (D. Mass. 2023)	54

<i>SEC v. World-Wide Coin Invs, Ltd.</i> , 567 F. Supp. 724 (N.D. Ga. 1983)	46, 47
<i>Strougo v. Barclays PLC</i> , 105 F. Supp. 3d 330 (S.D.N.Y. 2015)	40
<i>Teamsters Local 445 Freight Div. Pension Fund v. Dynex Cap. Inc.</i> , 531 F.3d 190 (2d Cir. 2008)	40, 41, 42
<i>United States v. Bilzerian</i> , 926 F.2d 1285 (2d Cir. 1991)	19, 21, 36
<i>Wilson v. Merrill Lynch & Co., Inc.</i> , 671 F.3d 120 (2d Cir. 2011)	29

STATUTES

15 U.S.C. § 77q(a)	9
15 U.S.C. § 78j.....	9
15 U.S.C. § 78m.....	43, 54
15 U.S.C. § 78t.....	54

REGULATIONS

<i>FAST Act Modernization and Simplification of Regulation S-K</i> , Release No. 33-10618, 2019 WL 1314887, 84 Fed. Reg. 12674 (SEC Apr. 2, 2019)	24
Regulation S-K Item 10, 17 C.F.R. § 229.10	23
Regulation S-K Item 105, 17 C.F.R. § 229.105	23
Regulation S-K Item 105, 17 C.F.R. § 229.303	59
Rule 10b-5, 17 C.F.R. § 240.10b-5	passim
Rule 13a-15, 17 C.F.R. § 240.13a-15	50, 51

OTHER AUTHORITIES

<i>Statement on Auditing Standards No. 1</i> , American Institute of Certified Public Accountants (1973)	45
<i>Certification of Disclosure in Companies' Quarterly and Annual Reports</i> , Rel. No. 33-8124, 2002 WL 31720215, 67 Fed. Reg. 57276, (SEC Aug. 29, 2002)	50
<i>Commission Statement and Guidance on Public Company Cybersecurity Disclosures</i> , Rel. Nos. 33-10459, 34-82746; 2018 WL 993646 (SEC Feb. 21, 2018)	55

<i>Statement of Financial Accounting Concepts No. 8,</i> Financial Accounting Standards Board, December 2021	50
<i>In the Matter of Altaba, Inc. f/d/b/a YAHOO!, Inc.,</i> Rel. No. 34-83096, 2018 WL 1919547 (SEC Apr. 24, 2018)	55
<i>Modernization of Regulation S-K Items 101, 103 and 105,</i> Rel. No. 34-89670, 2020 WL 5076727 (SEC Aug. 26, 2020)	24
<i>Plain English Disclosure,</i> Rel. No. 33-7497, 1998 WL 36880 (SEC Jan. 28, 1998),.....	24
<i>Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices,</i> Rel. No. 34-15570, 1979 WL 173674 (SEC Feb. 15, 1979)	44, 48
<i>Statement of Management on Internal Accounting Control,</i> Rel. No. 34-16877, 1980 WL 20857 (SEC June 6, 1980).....	44, 48
<i>Updated Staff Legal Bulletin No. 7: Plain English Disclosure,</i> 1999 WL 34984247 (SEC June 7, 1999).....	24

Plaintiff, the Securities and Exchange Commission (“SEC” or “Commission”), respectfully submits this opposition to the motion to dismiss the Amended Complaint filed by Defendants, SolarWinds Corporation (“SolarWinds” or the “Company”) and Timothy G. Brown (“Brown”) [ECF No. 88]. For the reasons stated below, the Court should deny Defendants’ motion in its entirety.

PRELIMINARY STATEMENT

Public companies and their officers cannot make public statements claiming to follow practices that are important to investors while knowing that they pervasively fail to do so. That is the essence of this case. SolarWinds and Brown claimed in multiple public forums that SolarWinds employed specific cybersecurity practices such as granting access to computer systems on a “least privilege necessary basis.” Amended Complaint [ECF No. 85] (“AC”) ¶ 181. But internally they admitted that the Company failed to follow the “least privilege necessary” practice because it had widespread access control problems (including granting elevated permissions to “non-privileged users”) and had determined that, “[a]ccess and privilege to critical systems/data is inappropriate.” *See* AC ¶¶ 182, 192. The most egregious examples of these affirmative false statements were in the Security Statement publicly posted on SolarWinds’ website. The numerous, material, false representations in the Security Statement could alone support the SEC’s fraud claims. But, as discussed below, there is much more.

In their brief, despite professing to accept the Amended Complaint’s factual allegations as true, Defendants mainly seek to dismiss this case by disputing the factual allegations or recasting the allegations in the light most favorable to Defendants. The Court should not indulge Defendants’ attempts to argue facts and inferences on a motion to dismiss.

As described in the Amended Complaint, from at least October 2018 through at least January 12, 2021 (the “Relevant Period”), Defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, recognized and documented the Company’s long-standing, pervasive, and material cybersecurity deficiencies. Nevertheless, they made public statements that directly contradicted the internal assessments and omitted the risks those deficiencies posed. Through these statements, and an overall scheme to portray SolarWinds as having a stronger cybersecurity posture than it did, SolarWinds and Brown misled the investing public.

SolarWinds and/or Brown made materially false and misleading statements and omissions in at least three types of public disclosures (*Id.* ¶ 6):

- a) Statements that purported to describe the Company’s cybersecurity practices and policies, including a “Security Statement” posted to the Company’s website throughout the Relevant Period;
- b) Form S-1 and S-8 Registration Statements and periodic reports filed with the SEC throughout the Relevant Period; and
- c) A Form 8-K filed with the SEC on December 14, 2020 regarding the massive SUNBURST cybersecurity incident that impacted SolarWinds’ Orion software platform.

The true state of SolarWinds’ cybersecurity practices, controls, and risks ultimately came to light only following a massive cyberattack—which exploited some of the very cybersecurity deficiencies that Brown had been warned about—and which impacted thousands of SolarWinds’ customers. That attack, termed SUNBURST, compromised SolarWinds’ flagship product, the Orion software platform. SolarWinds disclosed the SUNBURST attack in a Form 8-K on December 14, 2020, after its customer, Mandiant,¹ identified the malicious code and informed SolarWinds. Contrary to Defendants’ claims, the SEC is not re-victimizing SolarWinds for being hacked. Rather, the SUNBURST attack is just one part of a broader case involving fraud, control,

¹ Mandiant is referred to in the Amended Complaint as Cybersecurity Firm C.

and disclosure violations that began with SolarWinds’ October 2018 initial public offering—well before the SUNBURST attack.

The Amended Complaint contains detailed allegations about SolarWinds’ and Brown’s materially misleading statements, omissions, and actions. That conduct violated the antifraud and reporting provisions of the Securities Act of 1933 (“Securities Act”) and Securities Exchange Act of 1934 (“Exchange Act”). The same poor cybersecurity practices that SolarWinds and Brown schemed to conceal also constituted violations of the Exchange Act’s internal controls provisions. And although Defendants claim that this section only relates to controls relating to financial statements, case law and longstanding interpretive guidance make clear it relates to controls designed to ensure management is protecting a company’s assets. Finally, SolarWinds’ failure to maintain effective processes for elevating information, including information about cyberattacks, to its disclosure committee violated Exchange Act Rule 13a-15(a). Through his actions and misstatements, Brown not only committed securities fraud, but also aided and abetted SolarWinds in violating all these provisions. For these reasons, and the reasons explained below, the Court should deny Defendants’ motion to dismiss.

SUMMARY OF ALLEGATIONS

A. General Background

During the Relevant Period, SolarWinds designed and sold network monitoring software used by many businesses, as well as state, federal, and foreign governments, to manage their computer systems. *See* AC ¶¶ 4, 43. SolarWinds’ flagship product during the Relevant Period was the Orion information technology infrastructure and management suite of products. *Id.* ¶¶ 43-44. Orion accounted for 45% of the Company’s revenue in the first nine months of 2020. *Id.* ¶ 44. SolarWinds considered Orion to be one of its “crown jewels,” a term used by Brown and others to describe assets that, if compromised, could have a material impact on the Company. *Id.*

B. SolarWinds and Brown Made Misleading Public Statements Regarding SolarWinds’ Cybersecurity Practices.

1. Brown Drives SolarWinds to Post the False Security Statement.

When Brown joined SolarWinds in July 2017, he realized that the Company’s cybersecurity posture was poor. *See id.* ¶ 5. He also realized that SolarWinds lacked public security policies it could use to assuage customers’ concerns about cybersecurity, and that this lack of policies was costing the Company business. *Id.* So, working with others at SolarWinds, he began a scheme and course of business to mislead the public about the quality of the Company’s cybersecurity practices by posting a “Security Statement” and making other public statements that claimed SolarWinds was following good cybersecurity practices, even though Brown and others at SolarWinds knew this was false. *Id.* From almost the moment the Security Statement was published, SolarWinds recognized that it was materially false and misleading, and worked to conceal its falsity from the public. *See id.* ¶¶ 5, 10, 56-65, 117.

SolarWinds’ Security Statement remained publicly available on its website, virtually unchanged, throughout the Relevant Period. *See id.* ¶ 71. The Security Statement contained multiple, specific, materially false and misleading statements—assuring that SolarWinds followed well-recognized cybersecurity practices—when, in fact, the Company’s cybersecurity practices fell significantly short of those assurances. *See id.* ¶¶ 7, 72. These false statements and omissions included, among other things, claiming compliance with the widely used and internationally recognized National Institute of Standards and Technology Cybersecurity Framework (“NIST Cybersecurity Framework”) for evaluating cybersecurity practices. *See id.* ¶¶ 74-78. The Security Statement also misrepresented that SolarWinds followed four specific cybersecurity practices: (1) using a secure development lifecycle when creating software for customers; (2) employing network monitoring, (3) having strong password protection; and (4)

maintaining robust access controls. *See id.* ¶¶ 72, 77. Brown also made numerous misleading statements in SolarWinds-approved press releases, blog posts, podcasts, and presentations related to SolarWinds’ cybersecurity practices, in which he repeatedly stressed the importance SolarWinds placed on cybersecurity while knowing that SolarWinds’ practices were deficient. *See id.* ¶¶ 138-144, 156, 215-217, 219-225.

2. SolarWinds Made False Risk Disclosures in Its SEC Filings.

SolarWinds’ SEC filings similarly concealed the Company’s poor cybersecurity practices. SolarWinds’ sole cybersecurity disclosure in its October 18, 2018 Form S-1 for its initial public offering was generic and hypothetical. It stated “[i]f we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches,” negative impacts could occur. *See id.* ¶¶ 239-240. These general warnings were then repeated verbatim in each of SolarWinds’ periodic SEC filings during the Relevant Period, despite both the ongoing failures to meet its own Security Statement and the increasing red flags that SolarWinds had already been subject to an attack. *Id.* ¶¶ 242-245.

C. SolarWinds and Brown Failed to Disclose Red Flags and Warning Signs of a Cyberattack Leading up to the Revelation of the SUNBURST Cyberattack.

1. Defendants Failed to Adequately Respond to Warnings of a Security Gap.

Starting in June 2018, and continuing for months, a SolarWinds employee, Network Engineer D, repeatedly warned of a “security gap” in SolarWinds Virtual Private Network (“VPN”) setup. *Id.* ¶¶ 201-210. Despite the repeated warnings, Brown and SolarWinds failed to remediate the security gap. *Id.* ¶¶ 211-212. Then, in January 2019, the threat actors responsible for the SUNBURST cyberattack accessed SolarWinds’ corporate VPN, exploiting that exact VPN security gap. *See id.* ¶¶ 254-258.

2. The Defendants Did Not Address Increasing Attacks.

Beginning in early 2020, SolarWinds and Brown learned of an increase in threats to its products and customers but did not disclose these increased risks in the Company's periodic filings or otherwise. *See id.* ¶¶ 260, 290-297. For example, during 2020, SolarWinds learned of multiple attacks involving access control problems against a critical segment of its customers known as Managed Service Providers ("MSP") but was unable to determine the attacks' source and did not disclose related details. *See id.* ¶¶ 125, 261-266.

Also, in June 2020, the Executive Office of the U.S. Trustee Program ("USTP")² notified SolarWinds about malicious activity by the Orion software after it had been installed on a trial basis by the agency in May 2020 and asked SolarWinds to investigate. *See id.* ¶¶ 267-269. SolarWinds determined that a portion of the Orion software was reaching out and attempting to provide information to an unknown website about the network on which it was located. *Id.* ¶ 270. SolarWinds was unable to determine the root cause of the attack, but internally Brown expressed concern that it might be a threat actor attempting to use Orion as part of a larger attack. *Id.* ¶¶ 272, 274. In October 2020, another SolarWinds customer, Palo Alto Networks ("Palo Alto"),³ notified the Company about malicious activity by Orion software, which included the same component of Orion that was involved in the attack on USTP reaching out to a website and downloading a malicious file. *See id.* ¶ 279. SolarWinds employees recognized and discussed internally that the activity was similar to the USTP incident. *Id.* ¶¶ 280-281. Despite linking the two incidents and theorizing that an attacker was using SolarWinds' flagship Orion product as a vehicle for a larger attack (*Id.* ¶ 286), SolarWinds and Brown disclosed nothing about these incidents to investors, and Brown did not elevate the incident under the Company's Incident

² USTP is referred to in the Amended Complaint as U.S. Government Agency A.

³ Palo Alto is referred to in the Amended Complaint as Cybersecurity Firm B.

Response Plan despite knowing that it implicated multiple customers. *Id.* ¶¶ 285-288.

Additionally, while SolarWinds did not learn the root cause of the USTP or Palo Alto attacks until Mandiant notified the Company in December 2020, it did discover many other cybersecurity problems that it could not promptly remediate and did not disclose. *Id.* ¶¶ 276-278.

At no point during the Relevant Period did SolarWinds disclose the numerous risks, vulnerabilities, and incidents affecting its products in its SEC filings or elsewhere. *See id.* ¶ 298.

D. Once SolarWinds Learned of the SUNBURST Attack, It Did Not Fully Disclose Its Known Impact.

After learning from Mandiant on December 12, 2020, that malicious code had been inserted into the Orion platform, Brown and other executives worked to prepare a Form 8-K announcing the vulnerability. *Id.* ¶ 308. On December 14, 2020, SolarWinds filed a Form 8-K with the SEC that disclosed the SUNBURST attack, but omissions of material facts from that disclosure created a materially misleading picture. The Form 8-K stated that SolarWinds was aware of a vulnerability that “could potentially allow” an attacker to compromise the server on which the Orion products run, but failed to disclose that SolarWinds was aware of at least three previous incidents (USTP, Palo Alto, and Mandiant) where attackers had actually utilized the vulnerability since at least May 2020. *Id.* ¶¶ 310-312.

In a Form 8-K filed with the SEC on January 12, 2021, SolarWinds disclosed additional information regarding the SUNBURST attack. This included that the Company had “identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST,” and provided additional information about the USTP and Palo Alto attacks discussed above, including the months in which they occurred. *Id.* ¶ 319. This information was known to Brown at the time of the December 14, 2020 Form 8-K, but he did not disclose it to anyone else involved in preparing the Form 8-K. *Id.*

ARGUMENT

SolarWinds and Brown argue that the Amended Complaint fails to state a claim for which relief may be granted. *See* ECF No. 89 (“Br.”) *passim*. Contrary to Defendants’ arguments, the SEC has sufficiently alleged fraud, reporting, internal accounting control, and disclosure control claims. The Court should deny Defendants’ motion.

I. Standard of Review

To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Courts deny motions to dismiss claims “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Indeed, a complaint is properly dismissed only, where, as a matter of law, “the allegations in a complaint, however true, could not raise a claim of entitlement to relief.” *Twombly*, 550 U.S. at 558. A court must accept as true all well-pled factual allegations in the complaint and draw all reasonable inferences in the plaintiff’s favor. *Iqbal*, 556 U.S. at 678; *see also In re Sanofi Sec. Litig.*, 87 F. Supp. 3d 510, 525-26 (S.D.N.Y. 2015) (Engelmayer, J.).

II. The Amended Complaint Sufficiently Alleges Fraud.

A. The Legal Standards Applicable to Securities Fraud Claims.

The Amended Complaint alleges violations of the antifraud provisions set forth in Exchange Act Section 10(b) (and Rule 10b-5, thereunder) and Securities Act Section 17(a). Securities Act Section 17(a) makes it unlawful, in the offer or sale of any security:

to employ any device, scheme, or artifice to defraud, or (2) to obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or (3) to engage

in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.

15 U.S.C. § 77q(a). Exchange Act Rule 10b-5 makes it unlawful in connection with the purchase or sale of any security:

To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

17 C.F.R. § 240.10b-5; *see also* 15 U.S.C. § 78j. Section 17(a)(1) and all provisions of Rule 10b-5 require proof of scienter; Sections 17(a)(2) and (3) only require proof of negligence. *See SEC v. Monarch Funding Corp.*, 192 F.3d 295, 308 (2d Cir. 1999) (citing *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1467 (2d Cir. 1996)); *SEC v. Ginder*, 752 F.3d 569, 574 (2d Cir. 2014).

Fraud claims are also subject to the heightened pleading requirements imposed by Rule 9(b) of the Federal Rules of Civil Procedure. Rule 9(b) provides that, “[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally.” Fed. R. Civ. P. 9(b). Importantly, although “the SEC must meet the particularity standard under Rule 9(b), it need not satisfy the pleading requirements under the Private Securities Litigation Reform Act (‘PSLRA’).” *SEC v. China Ne. Petroleum Holdings Ltd.*, 27 F. Supp. 3d 379, 387 (S.D.N.Y. 2014). Thus, the Court should **not** “take into account plausible opposing inferences,” as that is an evaluation only done in PSLRA cases. *See SEC v. DiMaria*, 207 F. Supp. 3d 343, 354 (S.D.N.Y. 2016) (citing cases including *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 323 (2007)). But, throughout their brief, Defendants ask the Court to credit their inferences, interpretations, and even factual arguments, and rely on cases adjudicated under the PSLRA.

B. The Amended Complaint Sufficiently Alleges Misstatement Liability Under Rule 10b-5(b) and Section 17(a)(2).

The SEC has sufficiently alleged that SolarWinds and/or Brown made materially false and misleading statements about SolarWinds' cybersecurity practices. *First*, in the Security Statement, they made affirmative misrepresentations that SolarWinds followed specific cybersecurity practices they knew it did not follow. *Second*, SolarWinds made risk disclosures, substantially assisted by Brown, whose warnings not only incorporated the false Security Statement, but also failed to convey the specific risks faced by SolarWinds as opposed to the generic risks faced by any company. This left investors with a materially misleading picture of the actual risk of investing in SolarWinds. *Third*, SolarWinds' December 14, 2020 Form 8-K, which Brown approved for technical accuracy, misled investors about the scope of the SUNBURST attack because it omitted information about prior exploitations of that same problem over the preceding six months. Defendants attack these allegations largely by disputing facts alleged in the Amended Complaint or asking the Court to draw inferences in their favor, neither of which is appropriate in the context of a motion to dismiss. The SEC's allegations are more than sufficient to support misstatement claims under Section 17(a)(2) and Rule 10b-5(b).

1. The Security Statement's Representations Were False and Misleading.

SolarWinds and Brown made numerous materially false and misleading statements regarding SolarWinds' cybersecurity practices in the Security Statement that SolarWinds posted on its public website, and maintained there for years while knowing it was false and misleading. *See, e.g.*, AC ¶¶ 71-72. Nevertheless, Defendants argue that, notwithstanding extensive allegations in the Amended Complaint based on SolarWinds' contemporaneous internal communications, the Court should conclude that the statements in the Security Statement are not

materially misleading based on SolarWinds’ preferred interpretation of the underlying communications. *See* Br. at 21-34.

As an initial matter, the SEC asserts, and the Defendants do not dispute, that false statements on websites can lead to securities law liability. *See SEC v. Enters. Solutions, Inc.*, 142 F. Supp. 2d 561, 577 (S.D.N.Y. 2001) (granting summary judgment against CEO and President of publicly traded company for, *inter alia*, materially false statements on the company’s website); *SEC v. DCI Telecomms.*, 122 F. Supp. 2d 495, 499-500 (S.D.N.Y. 2000) (allegations that “Defendants filed false financial statements with the SEC, hyped them in annual reports, press releases and on DCI’s website” were sufficient to sustain fraud claims); *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1207, 1217 (N.D. Ga. 2019) (denying motion to dismiss complaint that alleged false cybersecurity statements on company’s website); *see also In re Carter-Wallace Inc. Sec. Litig.*, 150 F.3d 153, 156 (2d. Cir. 1998) (“market professionals generally consider most publicly announced material statements about companies, thereby affecting stock market prices”) (cleaned up); *SEC v. AT&T, Inc.*, 626 F. Supp. 3d 703, 761 (Engelmayer, J.) (“The total mix of information includes all information that is reasonably available to the public.”) (cleaned up).

As discussed below, Defendants’ arguments fail to accept as true all well-pled factual allegations in the complaint and draw all reasonable inferences in the plaintiff’s favor. *See Iqbal*, 556 U.S. at 678. That in itself is sufficient grounds for the Court to reject Defendants’ motion to dismiss as inconsistent with the standard of review. Nevertheless, reviewing the specific misrepresentations also demonstrates the sufficiency of the Amended Complaint.

a. SolarWinds Misleadingly Claimed to “Follow” the NIST Cybersecurity Framework.

In its Security Statement, SolarWinds claimed to “follow[] the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security

incidents.” *See* AC ¶ 74. In claiming to “follow” the NIST Cybersecurity Framework, Brown and SolarWinds made a materially false and misleading statement or omission by not revealing how poorly SolarWinds fared on multiple internal assessments related to that framework, including that many of the supposed “layered security controls” were not in place. *See id.* ¶¶ 76, 80, 84.

Defendants argue that claiming SolarWinds would “follow” the NIST Cybersecurity Framework does not imply that SolarWinds had achieved any particular level of success. *See* Br. at 23-24. In Defendants’ view, a person can “follow” a cake recipe by reading all the instructions to mix flour, eggs, sugar, and butter, and bake at 350° for thirty minutes even if they skip the eggs and sugar and put it in the oven for thirty minutes without turning on the oven. Even if that was what “follow” means here, and it was technically not false for Defendants to claim to “follow” the NIST Cybersecurity Framework, it was still materially misleading for them to make that claim while omitting poor scores and negative information from numerous assessments directly related to that framework. *See, e.g., In re Morgan Stanley Info. Fund Sec. Litig.*, 592 F.3d 347, 366 (2d Cir. 2010) (“The literal truth of an isolated statement is insufficient; the proper inquiry requires an examination of Defendants’ representations, taken together and in context....a disclosure about a particular topic, whether voluntary or required, ...must be complete and accurate.”) (cleaned up); *Kleinman v. Elan Corp. plc*, 706 F.3d 145, 153 (2d Cir. 2013) (“veracity of a statement or omission is measured not by its literal truth, but by its ability to accurately inform rather than mislead prospective buyers”) (quotation omitted); *SEC v. Gabelli*, 653 F.3d 49, 57 (2d Cir. 2011) (“so-called ‘half-truths’—literally true statements that create a materially misleading impression—will support claims for securities fraud”); *Macquarie Infrastructure Corp. v. Moab Partners, L.P.*, No. 22-1165, --- U.S. ---, 2024 WL 1588706, at *4 (U.S. Apr. 12,

2024) (misleading for child to tell his parents that he had dessert but omit that “dessert” was an entire cake).

Defendants do not deny that they received scores of “0” (no evidence/unassessed) and “1” (ad hoc/inconsistent) in the areas discussed in the Amended Complaint but argue that these low scores not “pervasive” in light of other internal assessments from later in the Relevant Period. *See* Br. at 24. Not only does this represent an improper attempt to weigh the facts at the motion to dismiss stage, but whether later assessments showed improvement in certain areas has no bearing upon whether the statements from earlier in the Relevant Period were materially misleading when made. *See* AC ¶¶ 83-88 (0s and 1s at time of October 2018 IPO), 89-91 (1s and 2s as of August 2019).

b. SolarWinds Evaluated Its Cybersecurity Using the NIST 800-53 Framework But Failed to Disclose the Problems It Found.

Defendants misconstrue the Amended Complaint’s allegations about NIST 800-53. NIST 800-53 is promulgated by the U.S. Department of Commerce’s National Institute for Standards and Technology. It provides a set of security and privacy controls that organizations can use to protect against cyberattacks and other threats.⁴ The SEC and the Defendants agree that SolarWinds used NIST 800-53 as part of its cybersecurity assessments. Br. at 25; AC ¶ 95. The Amended Complaint refers to a FedRAMP / NIST 800-53 assessment because those are the terms used in the documents that SolarWinds provided to the SEC.⁵ Regardless of why that evaluation was conducted, or what methodology it used, *it revealed many, glaring, organization-wide failures*. AC ¶¶ 98-102, 129-130, 153, 158, 170-171, and 193-194. Thus,

⁴ *See* <https://csrc.nist.gov/pubs/sp/800/53/r4/upd3/final> (last accessed April 17, 2024).

⁵ *Compare* Exhibit 1 to Declaration of William Bradley Ney (“Ney Decl.”) at p 1 (Title of attachment is FedRAMP_Security_Controls_Baseline as of 06282019.xlsx); *with* p. 4 (header on 6th column in that attachment is “NIST Control Description (From NIST SP 800-53r4 1/23/15).”

whatever the reason for that assessment, the result was material information showing that the cybersecurity claims in the Security Statement were false. SolarWinds’ arguments in response assert a factual dispute, at most, not a basis for dismissal.

c. SolarWinds Had “Significant Deficiencies” in Its Access Controls.

SolarWinds’ Security Statement is replete with specific, affirmative misrepresentations about its cybersecurity practices. Among these, it represented that the Company implemented strong access controls, including only providing access on a “least privilege necessary basis.” *See* AC ¶¶ 178-180. The Amended Complaint catalogues extensive and pervasive defects in SolarWinds’ access control policies over several years, including allowing elevated administrator access permissions for large swaths of users. *See id.* ¶¶ 181-200. Defendants argue that these documented failures do not present a “plausible basis” to show a “pervasive failure” of these controls, *see* Br. at 29, a plain factual disagreement that would require the Court to draw inferences in favor of SolarWinds, not the SEC as required.

Moreover, despite their best efforts, Defendants fail to demonstrate that the Amended Complaint’s allegations are implausible at all. SolarWinds’ own internal documents assessed that: (1) SolarWinds had “significant deficiencies” in access control (AC ¶¶ 199-200); (2) “access and privilege to critical systems data is inappropriate” (*Id.* ¶¶ 10(e), 192); and (3) SolarWinds had “No program/practice in place” for 23 of 43 access controls in its NIST 800-53 assessment. AC ¶ 193. While Defendants may wish to argue the factual issue of whether these and the many other access control failings identified in the Amended Complaint were “pervasive failures,” that factual dispute is not appropriately decided on a motion to dismiss.

For example, with respect to access to systems, Defendants assert the yellow color-coding on a document showing the need to “address the use of local administrator access to non-privileged users,” meant that work was “in progress.” *See* Br. at 29; AC ¶ 191. But Defendants’

assertion about has no basis in that document, which does not state anywhere that yellow coloring means “in progress.” *See* Declaration of Serrin Turner [ECF No. 91] Ex. 14 (such exhibits hereinafter cited as “Def. Ex.”) The most the allegations in the Amended Complaint and incorporated documents support is that yellow font means “that we need to do work” (Ney Decl. Ex. 2 at 43) or “Needs Improvement.” Def. Ex 16 at 3. It would be inappropriate on a motion to dismiss to credit the Defendants’ disputed interpretation of the record.

Additionally, the Amended Complaint alleges that SolarWinds broadly granted administrator privileges during the period. *See* AC ¶¶ 181-200, 202. That allegation standing alone would render materially false the Security Statement’s assertion that SolarWinds granted permissions on a “least privilege necessary basis.” *See id.* ¶¶ 179-187. If the Defendants disagree with that allegation, they can put forth factual evidence at summary judgment or at trial. But their disagreement with well-pled allegations cannot form the basis for a motion to dismiss.

Similarly, Defendants’ arguments that the defects in SolarWinds’ VPN policy were not implicated by the specific representations in the Security Statement are contradicted by the statement from a SolarWinds engineer describing the VPN issue as a “security gap” that was not repaired. *Compare* Br. at 29-30 with AC ¶¶ 201-213. This gap contradicted the Security Statement’s representation that access controls “define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.” *See id.* ¶ 179.

Indeed, another court has already found that many of the same specific claims in the Security Statement that the SEC alleges were false constitute actionable misstatements under Rule 10b-5. *See In re SolarWinds Corp. Sec. Litig.*, 595 F. Supp. 3d 573, 587 (W.D. Tex. 2022) (denying motion to dismiss misstatement claims predicated on SolarWinds and Brown’s assertions that SolarWinds “segmented its networks using ‘Role Based Access controls,’”

provided security training, and “adhered to a password policy.”). And at least one other court has found misrepresentations related to similar policies actionable. *See In re Equifax*, 357 F. Supp. 3d at 1219 (denying motion to dismiss due in part to false portrayals of strong cybersecurity by a company that “failed to implement adequate authentication measures to ensure that parties attempting to access its networks were authorized to do so.”)

d. SolarWinds’ Own Documents Show It Did Not Follow a Secure Development Lifecycle.

SolarWinds’ Security Statement and other public disclosures stated that it followed a Secure Development Lifecycle (“SDL”) methodology that, in turn, “follows standard security practices,” which require “Continuous Training,” “Threat Modelling,” and “Security Testing.” AC ¶¶ 110-114. SolarWinds’ internal documents showed rampant SDL failures. *See id.* ¶¶ 115-135. In their brief, Defendants argue that the underlying documents cited in the Amended Complaint do not support the allegations. *See Br.* at 25-27.

For example, Defendants argue that the internal NIST Cybersecurity Framework scorecard cited in the Amended Complaint showed evidence that a score of “2” (out of 5) on a July 2019 internal assessment showed that an SDL was in place, just with some missing elements. *See Br.* at 25; AC ¶ 128. Again, Defendants are seeking an inference from this document in their favor, not the SEC’s. Moreover, that is far from the SEC’s only allegation about SolarWinds’ failure to comply with an SDL. Other documents show training and threat modelling being rated as 0 or 1 (AC ¶124); that “[n]o threat modelling nor analysis [was] performed as part of any process....” (*Id.* ¶127); and there was “not a security training/awareness program in place.” (*Id.* ¶129). Exactly how flawed, or non-existent, this made SolarWinds’ SDL process is a factual dispute, but there is a plethora of well-founded allegations that Defendants’ representation that SolarWinds followed an SDL was materially misleading. *See id.* ¶¶120-133;

see also Bricklayers & Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd., 866 F. Supp. 2d 223, 243 (S.D.N.Y. 2012) (alleged “half-truths” regarding safety inspections and training programs sufficient to allege fraud claim) (citing *Gabelli*, 653 F.3d at 57)).

Similarly, SolarWinds contests the SEC’s interpretation of documents concerning SolarWinds’ penetration testing, another aspect of the SDL. SolarWinds’ internal documents showed multiple defects in SolarWinds’ penetration testing procedures that contradicted its representation in the Security Statement that SolarWinds followed standard security practices. *See* AC ¶¶ 120-122. SolarWinds argues that these documents show, at most, that SolarWinds “failed to follow certain aspects” of the SDL. *See* Br. at 26-27. As with its other arguments, these amount to impermissible attempts to draw inferences in Defendants’ favor. Additionally, the specific allegations show the lack of several testing procedures, not simply a questioning of “certain aspects” of them. *See, e.g.*, AC ¶ 121 (“No formalized testing. Identify and integrate penetration testing into product development phases”).

e. SolarWinds’ Own Documents Show Pervasive Network Monitoring Failures.

SolarWinds’ Security Statement represented that it followed industry-standard network monitoring processes, including change management, auditing and logging, and network security. *Id.* ¶ 148. In contrast, SolarWinds’ internal documents showed failing scores in several of these areas. *Id.* ¶¶ 151-154. Defendants argue that the cited internal documents show that SolarWinds had a program to improve network monitoring, *see* Br. at 27-28, but this again is an effort to contest the SEC’s factual allegations, not judge their legal sufficiency. Moreover, the NIST 800-53 assessment described above showed widespread failures in organizational network monitoring controls, contrary to Defendants’ argument that the document only addressed FedRAMP compliance for certain SolarWinds products. *Compare Id.* ¶148 (claiming that

“Network components, workstations, applications and any monitoring tools are enabled to monitor user activity”) *with Id.* ¶ 153 (describing that monitoring was a “GAP” because SolarWinds had “no program” to monitor “atypical usage” and that SolarWinds also had no continuous monitoring program in place). *See also In re Equifax*, 357 F. Supp. 3d at 1219 (denying motion to dismiss where company “failed to establish mechanisms for monitoring its networks for security breaches”).

f. SolarWinds Had Pervasive Password Policy Violations.

The Security Statement represented that it not only had, but “enforce[d]” a “strong password policy,” including use of “best practices.” *See* AC ¶¶ 159-162. As explained in the Amended Complaint, however, SolarWinds had widespread failures in enforcing and complying with its policy. *See id.* ¶¶ 163-173. Defendants argue that this represents gaps in execution rather than a pervasive failure. *See* Br. at 29. Absent other circumstances, a single gap in execution of a password policy may not render a statement that a company follows a strong password policy materially misleading. But here, the SEC has alleged numerous failures that were not just individual instances of an employee choosing a non-compliant password, but organizational-level failures to have controls and systems in place regarding the supposed password policy. AC ¶¶ 167-171. This included SolarWinds using its own Cloud products internally, even though in those products “[p]asswords have no specific parameters, as stated in the IT guidelines”; and ‘Passwords are able to be reused and are not changed at a set number of days.’” *Id.* ¶169.

g. SolarWinds’ Cybersecurity Problems Were Systemic.

Defendants argue that the Amended Complaint wrongly describes SolarWinds’ cybersecurity issues as systemic. *See* Br. at 31-33; *see also* AC ¶ 226. As discussed above, the issues catalogued in the Amended Complaint include organization-wide problems with access controls, network monitoring, and more. To read all of the problems catalogued in the Amended

Complaint as isolated incidents would not only require drawing multiple inferences in Defendants' favor, but it would also deny the great weight of the allegations that, viewed together and in context, demonstrates a state of cybersecurity affairs far different than the picture that SolarWinds painted in its public statements.

SolarWinds also criticizes the Amended Complaint's citation of Brown's internal presentation stating that the "current state of our security leaves us in a very vulnerable state for our critical assets" (*id.* ¶ 227), by claiming that because this statement in the October 2018 presentation is in yellow font, it means that "significant improvement has been made." Br. at 32. But there is no basis in the Amended Complaint or the document (Def. Ex. 12) for Defendants' claim that yellow font means "significant improvement has been made." As described above, the only inference supported by the record is that yellow font means "we need to do work" or "Needs Improvement." Again, Defendants are trying to contest facts, but drawing all inferences in the SEC's favor, the allegations show pervasive and systemic cybersecurity problems.

2. The False Statements in the Security Statement Were Material.

The Second Circuit has declared that materiality is "especially well suited for jury determination," *United States v. Bilzerian*, 926 F.2d 1285, 1299 (2d Cir. 1991). This makes sense as materiality is a "fact-specific inquiry" that "depends on the significance the reasonable investor would place on the withheld or misrepresented information." *See also Basic Inc. v. Levinson*, 485 U.S. 224, 240 (1988). Accordingly, "a complaint may not properly be dismissed...on the ground that the alleged misstatements or omissions are **not** material unless they are **so obviously unimportant** to a reasonable investor that reasonable minds could not differ on the question of their importance." *Ganino v. Citizens Utils. Co.*, 228 F.3d 154, 162 (2d Cir. 2000) (cleaned up) (emphasis added).

The Amended Complaint sufficiently alleges that Defendants' misstatements regarding SolarWinds' cybersecurity practices were material. The stark contrast between the pervasive positive claims in the Security Statement and the pervasive negative internal assessments is self-evidently material. Additionally, as discussed below, (1) multiple analysts who followed SolarWinds' stock during the relevant period, (2) Brown, and (3) SolarWinds' CIO all expressed in various ways the importance and significance of the assertions in the Security Statement for SolarWinds and/or its investors.

A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' security. Securities analysts covering SolarWinds stated that knowledge of the true state of its cybersecurity practices would have been material. AC ¶¶ 105-106. This is not only true for SolarWinds' overall cybersecurity, but analysts specifically confirmed the importance and materiality of misrepresentations about SDL (*id.* ¶¶ 137, 144-145); network monitoring (*id.* ¶ 157); and access control violations such as the expansive use of administrator privileges (*id.* ¶ 214).

Likewise, Brown emphasized the importance of cybersecurity in public statements, underscoring its materiality to investors. *Id.* ¶¶ 107-108. Brown specifically described the importance of protecting "crown jewel" assets using an SDL process, even calling a failure to protect "crown jewel" assets an "extinction event." *Id.* ¶¶ 138-141. Brown also publicly stressed the importance of network monitoring (*id.* ¶ 156); following password policies (*id.* ¶¶ 175-177); and maintaining strong access controls (*id.* ¶¶ 215-217).

Additionally, in her January and June 2018 self-performance assessments, SolarWinds' Chief Information Officer essentially confessed and confirmed "identity and access

management” and “security standards” as two deficiencies that were material, when she stated that they could adversely impact SolarWinds’ “IPO valuation.” *Id.* ¶ 218.

Further support for the materiality of these misstatements and omissions come from the allegations about the drop in SolarWinds’ stock of more than 16% immediately after the disclosure of the SUNBURST attack in SolarWinds’ December 14, 2020 8-K, with an additional 8% drop the next day and a total drop of 35% by the end of the month. *See id.* ¶ 318. Although the December 14, 2020 8-K was incomplete for the reasons stated in the Amended Complaint, still the magnitude of this drop, construed in the SEC’s favor, supports an inference of materiality. *See Bilzerian*, 926 F.2d at 1298 (“[W]hether a public company’s stock price moves up or down or stays the same...does not establish the materiality of the statements made, though stock movement is a factor the jury may consider relevant.”).

Furthermore, a court already found that some of these same misstatements were material for the purposes of a motion to dismiss, in part because the allegations concerned the representations in the Security Statement, not the fact of the breach. *See In re SolarWinds Corp.*, 595 F. Supp. 3d at 587-88 (holding that plaintiffs “have alleged separate facts that the cybersecurity measures at the company were not as they were portrayed” and that “Plaintiffs have adequately alleged misleading material statements”).

Likewise, in *In re Equifax*, 357 F. Supp. 3d at 1226-1227, the district court held that the complaint sufficiently alleged materially misleading statements related to Equifax’s security practices, which, like those here, were alleged to contradict facts known to the company at the time. *See id.* at 1219 (“Given the dangerously deficient state of Equifax’s cybersecurity, the Court concludes it was false, or at least misleading, for Equifax to tout its advanced cybersecurity protections”). That court further held that plaintiffs sufficiently alleged materiality

regarding Equifax’s data security statements considering the importance of data security to Equifax’s business. *Compare id.* at 1224 (“Since data security plays an important part of a business such as Equifax, investors would be even more likely to find these types of representations important in making their investment decisions.”) *with* AC ¶ 103 (noting cybersecurity representations were particularly important for SolarWinds because it develops software that customers use to manage their computer networks). The Amended Complaint thus sufficiently pleads material misstatements and omissions in the Security Statement.

3. Brown’s Other Public Statements Were Materially False and Misleading.

The Amended Complaint cites many public statements by Brown, *e.g.*, company-approved press releases, blog posts, podcasts, and presentations, in which Brown touts SolarWinds’ cybersecurity practices. *See id.* ¶¶ 219-235. Defendants seek to dismiss these statement as “puffery.” Br. at 31. Puffery encompasses “statements [that] are too general to cause a reasonable investor to rely upon them,” and thus “cannot have misled a reasonable investor.” *ECA, Local 134 IBEW Joint Pension Tr. of Chicago v. JP Morgan Chase Co.*, 553 F.3d 187, 206 (2d Cir. 2009). But “[w]hile statements containing simple economic projections, expressions of optimism, and other puffery are insufficient, defendants may be liable for misrepresentations of existing facts.” *Novak v. Kasaks*, 216 F.3d 300, 315 (2d Cir. 2000) (citations omitted); *see also In re Virtus Inv. Partners, Inc. Sec. Litig.*, 195 F. Supp. 3d 528, 537 (S.D.N.Y. 2016) (statements that “contradict[ed] facts that [we]re known to” speaker were not puffery). The Amended Complaint sufficiently alleges that Brown’s representations about the Company’s cybersecurity practices in public statements were not merely optimistic, but factual and contradicted by SolarWinds’ actual cybersecurity practices. *See, e.g.*, AC ¶ 222 (SolarWinds “makes sure everything is backed by sound security processes, procedures and standards”), ¶ 224

(“SolarWinds’ commitment to high security standards”). Such claims were found to be actionable in *In re Equifax*, 357 F. Supp. 3d at 1224, where the court rejected puffery arguments for statements including claims the company employed “advanced security protections” and was “committed to data security” because:

the Defendants repeatedly stated that cybersecurity, an important aspect of their business, was a top priority for senior management, despite the fact that Equifax failed to employ some of the most elementary cybersecurity practices. Even if, in a vacuum, each of these statements seems like a meaningless, corporate vaguery, when taken together a reasonable investor would rely upon them to conclude that Equifax made cybersecurity a serious priority.

Moreover, even if some of Brown’s statements in blogs and podcasts are puffery, they are still relevant to materiality and scienter, and when considered in context with the other specific statements, there is no basis to dismiss the fraud claims on “puffery” grounds. *See In re SolarWinds Corp.*, 595 F. Supp. 3d at 587 (considering Defendants’ statements together and rejecting puffery argument); *see also In re BHP Billiton Ltd. Sec. Litig.*, 276 F. Supp. 3d 65, 79 (S.D.N.Y. 2017) (even if “certain statements, viewed in isolation, may be mere puffery, when the statements are made repeatedly in an effort to reassure the investing public about matters particularly important to the company and investors, those statements may become material to investors.” (cleaned up)); *see also Richman v. Goldman Sachs Grp., Inc.*, 868 F. Supp. 2d 261, 279 (S.D.N.Y. 2012) (“repeated assertions” were not mere puffery).

4. SolarWinds’ Generic Risk Disclosures in Its SEC Filings Were False and Misleading.

a. Companies Cannot Rely on Generic Disclosures.

Securities registration statements and periodic SEC filings, such as the Forms S-1, 10-K, and 10-Q filed by SolarWinds, must include disclosures of material risks. *See* Regulation S-K, Item 10 [17 C.F.R. § 229.10] and Item 105 [17 C.F.R. § 229.105]. The SEC has long “eschewed ‘boiler plate’ risk factors that are not tailored to the unique circumstances of each registrant.”

See, e.g., FAST Act Modernization and Simplification of Regulation S-K, Release No. 33-10618 at 53 (Mar. 20, 2019), 2019 WL 1314887, at *22 [84 Fed. Reg. 12674, 12702 (SEC Apr. 2, 2019)]. The Commission’s 1998 guidance on presenting risk factors made this point explicitly:

If you include a risk factors section in your prospectus, you must write the risk factors in plain English and avoid “boilerplate” risk factors. We believe a discussion of risk in purely generic terms does not tell investors how the risk may affect their investment in a specific company. You should place any risk factor in specific context so investors can understand the specific risk as it applies to your company and its operations.

Plain English Disclosure, Rel. No. 33-7497, 1998 WL 36880, at *7 (SEC Jan. 28, 1998); *see also Updated Staff Legal Bulletin No. 7: Plain English Disclosure*, 1999 WL 34984247, at *2 (SEC June 7, 1999) (admonishing issuers to avoid “vague ‘boilerplate’ explanations that are imprecise and readily subject to different interpretations”). Contrary to this guidance, Defendants argue that SolarWinds’ generic risk disclosures were adequate. *See Br.* at 9-16. This is a fundamental disagreement between the parties. SolarWinds effectively argues that because (1) all technology companies are vulnerable to cyberattacks and (2) SolarWinds’ risk disclosures stated that it was vulnerable, the Company has met its disclosure duty. Not so.

The SEC disapprovingly discussed the use of generic risk disclosures when it adopted further amendments to Item 105 in 2020, stating:

[a]lthough Item 105 instructs registrants not to present risks that could apply generically to any registrant, and despite longstanding Commission and staff guidance stating that risk factors...should not be boilerplate, it is not uncommon for companies to include generic risks. ***Registrants often disclose risk factors that are similar to those used by others in their industry without tailoring the disclosure to their circumstances and particular risk profile.***

Modernization of Regulation S-K Items 101, 103, and 105, Rel. No. 34-89670, 2020 WL 5076727, at *29 (SEC Aug. 26, 2020) (emphasis added). The SEC then specifically discouraged this approach, admonishing that “[t]he presentation of risks that could apply generically to any registrant or any offering is discouraged.” *Id.* at *59.

Courts have similarly held that the use of generic, boilerplate risk disclosures in the face of known, specific risks will not shield an issuer from liability. “A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor’s calculations of probability.” *Meyer v. Jinkosolar Holdings Co., Ltd.*, 761 F.3d 245, 251 (2d Cir. 2014); *see also SEC v. DeFrancesco*, ___ F. Supp. 3d ___, No. 23-cv-131 (JSR), 2023 WL 4631449, at *4 (S.D.N.Y. July 20, 2023) (general risk disclosure related to growth was inadequate when company knew of deteriorating business relationship with main customer). SolarWinds’ risk disclosures did not sufficiently warn investors that Brown and Company employees had determined that SolarWinds was facing specific, elevated risks because of its poor cybersecurity posture. *See* AC ¶¶ 1, 9, 11, 227, 240-246, 296-297.

b. SolarWinds’ Generic Disclosure that It Was “Vulnerable” to Cybersecurity Threats Failed to Provide Investors With Material Information About SolarWinds’ Specific Risk Profile.

Defendants argue that SolarWinds’ risk disclosures adequately disclosed the risk of cybersecurity incidents because they warned of the possibility of cybersecurity incidents that ultimately materialized. *See* Br. at 9-16. In doing so, Defendants place great emphasis on the fact that the risk disclosure said that SolarWinds was “vulnerable” to cybersecurity threats. Br. at 10. But Defendants admit the generic and boilerplate nature of the disclosure, noting that it merely disclosed that “[l]ike any technology-focused business, SolarWinds is vulnerable to the pervasive risk of cybersecurity attacks.” Br. at 4. Indeed, SolarWinds’ cybersecurity disclosure lumped cyberattacks in a laundry-list of risks alongside “natural disasters, fire, power loss, telecommunication failures...[and] employee or contractor theft or misuse.” AC ¶ 240.

SolarWinds’ risk disclosure is precisely the type of generic, industry-wide risk disclosure that the Commission specifically cautioned against in Item 105 and in the Plain English Disclosure rules discussed above. As described in the Amended Complaint, because of its

pervasive cybersecurity failings and increasing threats against its products and infrastructure, SolarWinds and Brown recognized, internally, that the Company was facing risks far greater than a generic, technology-focused business. *See id.* ¶¶ 227-229, 241, 246-247, 296. SolarWinds is correct in asserting that all technology companies are vulnerable to hackers, just like all companies that store large quantities of physical inventory are vulnerable to earthquakes. Yet a crystal chandelier company that has learned that 45 percent of its inventory is in a warehouse on top of a fault larger than the *San Andreas* cannot blithely assert that it is “vulnerable to earthquakes” in response to this information, especially if pared with references to precautions it falsely claims to be taking.

Likewise, SolarWinds cannot escape liability with a general reference to being vulnerable in the way that all technology companies are vulnerable, when (1) Brown had made a specific assessment that the Company’s security posture was so poor that it left its *critical assets* very vulnerable; (2) the Company had longstanding access control problems that were variously described as “significant deficiencies” and capable of affecting the entire Company’s valuation; (3) Brown and SolarWinds’ CIO had determined that “access and privilege to [the Company’s] critical systems/data [was] inappropriate”; and (4) there were multiple red flags of increasing problems at SolarWinds in 2020, including the linked USTP and Palo Alto attacks. *See id.* ¶¶ 192, 198, 227, 280.

Contrary to SolarWinds’ assertion, the issue is not whether it paired the modifier “very” with the word “vulnerable.” Br. at 15. The issue is that there were specific, pervasive, and longstanding cybersecurity problems within SolarWinds that were not conveyed by a generic disclosure that the Company was vulnerable to hackers (and natural disasters, fire, power loss, *etc.*). The omission of any reference to the Company-specific cybersecurity problems at

SolarWinds (such as its critical assets being highly vulnerable, or there being significant deficiencies in its access controls) rendered its risk disclosure materially misleading. SolarWinds repeated this misleading, generic risk disclosure in its quarterly and annual SEC filings. *Id.* ¶¶ 242-245, 298-301.⁶

c. The Cases Relied Upon by SolarWinds Did Not Involve Omission of Specific Material Risks.

Defendants rely on cases about cybersecurity risk disclosures that were found to be adequate under the circumstances. *See* Br. at 10-11. But those cases did not involve disclosures that omitted specific risks known by the Company at the time. *See In re Qudian Sec. Litig.*, No. 17-cv-9741 (JMF), 2019 WL 4735376 (S.D.N.Y. Sept. 27, 2019) (disclosure of risks relating to data security was not misrepresentation when it disclosed currently-known risks, including being under regulatory examination for potential violations of data security regulations); *In re Equifax*, 357 F. Supp. 3d at 1226-1227 (description that “could be vulnerable” found not to be misleading because it did not contradict or omit known facts); *compare In re Van der Moolen Holding N.V. Sec. Litig.*, 405 F. Supp. 2d 388, 400 (S.D.N.Y. 2005) (upholding allegations that a warning of employee misconduct was misleading when company knew, or was reckless in not knowing, that employees were violating regulations).

Unlike *In re Qudian* and *In re Equifax*, this case concerns SolarWinds making a generic disclosure, while failing to disclose specific, known “facts on the ground [that] would substantially affect a reasonable investor’s calculations of probability” of a material cyberattack against SolarWinds. *See Meyer*, 761 F.3d at 251; *see also In re Fannie Mae 2008 Sec. Litig.*, 742

⁶ These same misstatements, and the misstatements in the December 2020 8-K support the SEC’s false filing claims. *See SEC v. McNulty*, 137 F.3d 732, 741 (2d Cir. 1998) (false filing claim under Exchange Act § 13(a) does not require scienter); *see also SEC v. Koenig*, 469 F.2d 198, 200 (2d Cir. 1972) (“material omission” in SEC filings constituted violation).

F. Supp. 2d 382, 404–06 (S.D.N.Y.2010) (finding material misstatements sufficiently pled where Fannie Mae’s statements that its risk management operation was “appropriate” were made despite knowledge that their risk management system was inadequate); *cf. In re BP p.l.c. Sec. Litig.*, 843 F. Supp. 2d 712, 761 (S.D. Tex. 2012) (“Statements about the adequacy of risk management operations and capabilities may be false and misleading where the speaker knows, or should know, that such operations are inadequate to manage the risks a company faces”).

As described in the Amended Complaint, SolarWinds failed to disclose in its risk factors anything about the numerous problems that rendered the incorporated Security Statement false, or the linked attacks, red flags, and increasing problems in 2020. In combination, these facts, which were known to Defendants but not disclosed to investors and analysts, would have materially affected a reasonable investors’ assessment of the probability of a material incident.

Defendants also rely on cases from this Court outside the cybersecurity context involving whether a risk disclosure constituted meaningful cautionary language for purposes of the PSLRA safe harbor provisions (which do not apply here) or the common law “bespeaks caution” doctrine, which protects forward-looking statements made with sufficient cautionary language. *See Br.* at 10-11. Although the disclosures in those cases were held to have adequately disclosed the risks at issue, they involved more substantive cautionary language than the generic risk disclosures here. *See In re Sanofi*, 87 F. Supp. 3d at 536 (disclosure of “important factors” that could cause FDA denial); *Garnett v. RLX Tech. Inc.*, 632 F. Supp. 3d 574, 602 (S.D.N.Y. 2022) (detailed disclosure of changing Chinese regulatory treatment of e-cigarettes), *In re FBR Inc. Sec. Litig.*, 544 F. Supp. 2d 346, 361 (S.D.N.Y. 2008) (complaint premised on failure of compliance program controls rather than misleading statements about them).

Additionally, to apply the “bespeaks caution” doctrine, “the cautionary language must pertain to the specific risk that was realized.” *Garnett*, 632 F. Supp. 3d at 597 (quotation omitted); *see also Wilson v. Merrill Lynch & Co., Inc.*, 671 F.3d 120, 130 (2d Cir. 2011) (“The doctrine of bespeaks caution provides no protection to someone who warns his hiking companion to walk slowly because there might be a ditch ahead when he knows with near certainty that the Grand Canyon lies one foot away”) (quotation omitted); *Macquarie*, 2024 WL 1588706, at *4. The risk disclosures, and the Security Statements incorporated into them, did not fairly portray the risks SolarWinds faced. Thus, the generic disclosures in this case did not “precisely address the substance of the specific statement or omission that is challenged.” *In re Prudential Sec. Inc. Ltd. P’ships Litig.*, 930 F. Supp. 68, 72 (S.D.N.Y. 1996). Moreover, “cautionary language that is misleading in light of historical fact cannot be meaningful.” *Wilson*, 671 F.3d at 130 (quoting *Slayton v. Am. Express Co.*, 604 F.3d 758, 770 (2d Cir. 2010) (cleaned up)). This case involves misstatements of both present and historical facts, including in the false and misleading Security Statement representations about SolarWinds then-present security practices and the failure to disclose anything about the USTP and Palo Alto attacks. Thus, SolarWinds cannot escape liability through the cautionary language in the risk disclosures.

d. SolarWinds Presents a False Dichotomy Between Its Generic, Boilerplate Risk Disclosures and “Granular” Disclosures that Would Provide a “Roadmap” to Threat Actors.

Notwithstanding the SEC’s guidance against the use of boilerplate, industry-wide disclosures, SolarWinds defends its disclosures by making the unsubstantiated claim that anything more particular would consist of “granular” information on “internal problems” that would not be relevant to investors, *see* Br. at 12-13, or would involve providing a roadmap to threat actors. *See* Br. at 13-14. Defendants’ argument presents the Court with a false dichotomy that is unsupported by the well-pled facts in the Amended Complaint. This is not a case in which

only granular information was withheld. Rather, this is a case in which SolarWinds was aware of major, unremediated cybersecurity risks and vulnerabilities that threatened significant financial and reputational harm to the Company. The SEC is not asserting that each specific cybersecurity problem recited in the Amended Complaint needed to be individually disclosed. But, at a minimum, the categorical assessment of those issues, such as the fact that SolarWinds had significant deficiencies in access controls or that it had determined its critical assets were at heightened risk, needed to be disclosed to investors in some format beyond a generic warning applicable to all technology companies. If a company chooses to raise funds from investors in the public markets, it has an obligation to accurately inform them of the risk to their investment.

Defendants rely on several cases for the proposition that SolarWinds' cybersecurity problems were too granular to warrant disclosure. *See* Br. at 12-13. Those cases are distinguishable:

- *In re Intel Corp. Sec. Litig.*, No. 18-cv-00507-YGR, 2019 WL 1427660, at *13 n.17 (N.D. Cal. 2019) found that the company's risk disclosures were adequate to balance vague representations about the security features of its chips. SolarWinds' Security Statement was far more specific, and its problems far greater.
- *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 459 (S.D.N.Y. 2000) dealt with a failure to disclose internal assessments about weakness in its product line, a topic the company had not spoken about at all. In this case, SolarWinds did speak on cybersecurity, and it is indisputable that once it did those disclosures must be accurate. *See In re Morgan Stanley*, 592 F.3d at 366 ("when an offering participant makes a disclosure about a particular topic, whether voluntary or required, the representation must be complete and accurate") (cleaned up).
- *Ong v. Chipotle Mexican Grill, Inc.*, 294 F. Supp. 3d 199, 234 (S.D.N.Y. 2018) actually supports the SEC's position. There, the company made highly individualized disclosures about why its specific food-preparation practices placed it at higher risk than other companies. *See id.* at 235 ("disclosures regarding its risks...were company-specific and related to the direct risks it uniquely faced; there can be no argument that these were boilerplate statements").
- *In re Bank of Am. AIG Disclosure Sec. Litig.*, 980 F. Supp. 2d 564, 579 (S.D.N.Y. 2013) found a risk disclosure that the company was facing litigation over mortgage-backed security issues generally was sufficient disclosure of the risk of one particular suit. Here the

issue is not that SolarWinds did not forecast the specific SUNBURST attack, but that it presented an overall misleading picture of its susceptibility to such cyberattacks.

- *City of Austin Police Ret. System v. Kinross Gold Corp.*, 957 F. Supp. 2d 277, 303 (S.D.N.Y. 2013), dealt with an alleged failure to warn of the specific problems that derailed a project. This Court found the warnings sufficient to cover that specific problem. By contrast, here, the overall picture that SolarWinds presented to the investing public, through the Risk Disclosure and the Security Statement that it incorporated into it, was misleading.

Defendants argue that requiring further disclosure would be impractical because it would provide threat actors with a “roadmap” of “how” SolarWinds was vulnerable to attack. *See* Br. at 13-14. Contrary to SolarWinds’ argument, the Amended Complaint does not allege that SolarWinds failed to disclose “how” it was vulnerable to cybersecurity attacks but rather that SolarWinds’ disclosures as to its cybersecurity risks were misleading. Similarly, the SEC’s 2018 guidance regarding cybersecurity disclosures did not state that corporations should disclose the precise nature of their cybersecurity vulnerabilities, but that they should disclose material risks. *See* AC ¶ 248; *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, (“SEC 2018 Cybersecurity Release”), Rel. Nos. 33-10459, 34-82746; 2018 WL 993646, at *2 (SEC Feb. 21, 2018) (“it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.”). Moreover, it cannot be the case that a public company may publicly proclaim to follow a Secure Development Lifecycle, or other important cybersecurity practices, but claim that acknowledging that statement is pervasively false would impermissibly provide a roadmap to threat actors. Fear of threat actors cannot be perverted into a license to lie. Defendants’ argument thus fails.

5. The Information Omitted from the Risk Disclosures Was Material.

Defendants also argue that “no reasonable investor” would have found the omitted information from SolarWinds’ disclosures to be relevant to the “total mix” of information made available. *See* Br. at 15 (citing *Basic*, 485 U.S. at 231-32). But they cannot clear the high hurdle of dismissing a securities fraud claim on materiality grounds at the pleading stage. Contrary to Defendants’ argument, the Amended Complaint specifically alleges multiple specific facts sufficient to establish the materiality of the omissions, including specific statements from analysts who confirmed the materiality of many of the omitted details. *See* AC ¶¶ 241-244, 298-301. This includes an allegation that the representative of a major SolarWinds investor would have wanted to know about the linked USTP and Palo Alto attacks before deciding whether to go through with the investment. *Id.* ¶ 289.

Such omissions, after the Company had specifically chosen to speak, were materially misleading. *See Meyer*, 761 F.3d at 250 (“Even when there is no existing independent duty to disclose information, once a company speaks on an issue or topic, there is a duty to tell the whole truth.”); *see also Freudenberg v. E*Trade Fin. Corp.*, 712 F. Supp. 2d 171, 179 (S.D.N.Y. 2010) (“[O]nce corporate officers undertake to make statements, they are obligated to speak truthfully and to make such additional disclosures as are necessary to avoid rendering the statements made misleading”) (quotation omitted). The Court should not credit Defendants’ attempts to dismiss these undisclosed facts as immaterial “details.”

Similarly, Defendants cite cases in which this Court held that risk disclosures did not need to include precise estimates of the probability of risk when the overall risk was disclosed. *See* Br. at 15; *Kinross*, 957 F. Supp. 2d at 298 (not misleading to call ore “relatively hard” rather than “very hard” when terms were not industry terms of art); *In re ProShares Tr. Sec. Litig.*, 728 F.3d 96, 103 (2d Cir. 2013) (“diverge significantly” sufficiently close to “actual loss”); *Hill v.*

Gozani, 638 F.3d 40, 60 (1st Cir. 2011) (not required to call risk “serious” when “level of risk is unknown and the existence of a risk is disclosed”). These cases, however, acknowledge that disclosures that do not adequately disclose known facts relating to risk, as was the case here, are inadequate. *See, e.g., Kinross*, 957 F. Supp. 2d at 298 (“representations about due diligence anchored in specific factual claims may be actionable”); *Hill*, 638 F.3d at 60 (“generic and formulaic” statement of risk does not “insulate the speaker from liability”).

Furthermore, Defendants incorrectly argue that any misleading statements in the Security Statement about SolarWinds’ cybersecurity practices are not relevant to whether the risk disclosures were misleading because the risk disclosures did not discuss the security measures. *See Br.* at 15-16. But SolarWinds’ risk disclosures stated that it was vulnerable to cybersecurity incidents “despite our security measures.” *Br.* at 16; *see also* Def. Ex. 1 at 3. That reference to SolarWinds’ security measures essentially incorporates the Security Statement into the risk disclosures and makes them part of the total mix of information that “substantially affect a reasonable investor’s calculations of probability” of a breach. *Meyer*, 761 F.3d at 251; *see also Freudenberg*, 712 F. Supp. 2d at 190 (“statements touting risk management [that] were . . . juxtaposed against detailed factual descriptions of the Company’s woefully inadequate or non-existent credit risk procedures” were actionable misstatements); *Richman*, 868 F. Supp. 2d at 277 (complaint sufficiently alleged that Goldman’s statements touting its “extensive procedures and controls” for addressing “conflicts of interest” were actionable misstatements).

Defendants also cite cases in which risk disclosures were held sufficient to address the risk of a later cybersecurity breach. *See Br.* at 33-34; *In re Marriott Int’l, Inc.*, 31 F.4th 898, 903 (4th Cir. 2022) (finding no misrepresentation when Marriott made no representation about the “quality” of its cybersecurity practices); *In re Intel*, 2019 WL 1427660, at *9 (finding no liability

for marketing statements with “vague positive statements” regarding security practices); *In re Heartland Payments Systems, Inc. Sec. Litig.*, No. 09-cv-1043, 2009 WL 4798148, at *5 (D.N.J. 2009) (no liability when allegations premised upon fact of the breach). These cases are distinguishable because they involved allegations premised on the fact of a breach, in contrast to the specific, affirmative false statements about the “quality” of SolarWinds’ cybersecurity practices at issue here. *See In re SolarWinds Corp.*, 595 F. Supp. 3d at 588 (distinguishing *Heartland* due to allegations of misrepresentations of SolarWinds’ security practices); *In re Equifax*, 357 F. Supp. 3d at 1220-21 (distinguishing *Heartland* due to misleading security statements); *see also In re ValuJet, Inc. Sec. Litig.*, 984 F. Supp. 1472, 1477-78 (N.D. Ga. 1997) (statements touting “operational integrity” and safety were false given safety incidents).

6. SolarWinds’ Incomplete SUNBURST Disclosure in Its December 14, 2020 8-K Was Materially False and Misleading.

Defendants argue that SolarWinds’ December 14, 2020 Form 8-K disclosing the SUNBURST incident was not materially false or misleading. *See Br.* at 16-20. Again, Defendants’ arguments amount to factual disputes over the proper interpretation of the Form 8-K that are unsuited for a motion to dismiss. That Form 8-K described the impact of SUNBURST as theoretical, stating that it “could potentially allow an attacker to compromise the server on which the Orion products run;” considering “whether a vulnerability in the Orion monitoring products was exploited;” and claiming it was “still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited.” *See AC* ¶¶ 310-312. By that time, however, Brown had already concluded that the previous attacks were linked to SUNBURST. *Id.* ¶¶ 313-314. Accordingly, the Amended Complaint sufficiently alleges that the description of the risk was materially misleading.

Defendants argue that the statement that SUNBURST “could potentially ...compromise the server on which the Orion products run” was accurate because it was still investigating whether an attacker had “successfully exploited” SUNBURST by infiltrating networks rather than by inserting malicious code that could be used to infiltrate networks later as of the time of the December 14, 2020 Form 8-K. *See* Br. at 17-18. Even if the way Orion acted at USTP and Palo Alto is not considered an “infiltration” as SolarWinds used that term in the Form 8-K (which is a factual issue to be determined), it was still misleading by omission to fail to disclose those incidents, when SolarWinds (1) had previously concluded that the USTP attack was a “customer compromise” and an “attack that was successful” and (2) knew that the Palo Alto attack was a “breach” that involved the actual download of malicious files onto the customer’s Orion server. *See* AC ¶ 315. Additionally, because the USTP attack had taken place in May, the failure to disclose these incidents in the December 14, 2020 Form 8-K obscured the length of time the threat actors had been actively using SUNBURST to attack SolarWinds customers, another material fact. *Id.* Saying something could happen, when Brown and SolarWinds knew it already had, was materially misleading. Courts have repeatedly sustained such allegations. *See In re Van Der Moolen Holding*, 405 F. Supp. 2d at 400 (“to caution that it is only possible for the unfavorable events to happen when they have already occurred is deceit”) (citing cases).

Next, Defendants argue that the December 14, 2020 Form 8-K was not misleading because it disclosed that SolarWinds was still investigating whether any customers had been compromised and had recently hired a third-party cybersecurity firm to conduct the investigation. *See* Br. at 19. Regardless of whether SolarWinds was conducting a further investigation, it had an obligation to give accurate disclosures when speaking about the incident. *See, e.g., Meyer*, 761 F.3d at 250; *In re Morgan Stanley*, 592 F.3d at 366.

Lastly, Defendants argue that the Court should conclude that the failure to disclose the prior incidents in the December 14, 2020 Form 8-K was not material by comparing the immediate drop in SolarWinds' stock following the December 14, 2020 Form 8-K with the lesser drop following the January 12, 2021 Form 8-K. *See* Br. at 19-20. The relevant authorities, however, instruct that materiality involves an evaluation of multiple factors and is not limited to an analysis of stock price movement. *See Bilzerian*, 926 F.2d at 1298 (“[W]hether a public company’s stock price moves up or down or stays the same...does not establish the materiality of the statements made, though stock movement is a factor the jury may consider relevant.”); *Ganino*, 228 F.3d at 162 (the materiality element does not require a showing “that the investor would have acted differently if an accurate disclosure was made.”) (citation omitted).

Moreover, the two cases Defendants cite for this proposition—*In re Citigroup, Inc. Sec. Litig.*, 330 F. Supp. 2d 367 (S.D.N.Y. 2004), and *Beleson v. Schwartz*, 419 F. App’x 38 (2d Cir. 2011)—are inapposite. In *Citigroup*, this Court dismissed a securities fraud claim involving an alleged failure to disclose litigation risks from Enron-related transactions, finding plaintiffs had not sufficiently alleged that the risks were “material in the context of Citigroup’s overall business.” *In re Citigroup, Inc.*, 330 F. Supp at 378. Here, however, the risks are alleged to have had a significant negative effect on SolarWinds’ business. *See* AC ¶¶ 20, 318. *Beleson* involved a factual analysis *at summary judgment* of whether “the market was adequately informed of the dire nature of [the company’s] financial condition” by previous disclosure of large financial losses. *Beleson*, 419 F. App’x at 40. Thus, these cases do not support Defendants’ position.

C. The Amended Complaint Sufficiently Alleges Scheme Liability.

Courts collectively refer to Rule 10b-5(a) and (c) and Securities Act Section 17(a)(1) and (3) as encompassing scheme liability. “Essentially the same elements are required under” these sections, except that Section 17(a)(1) and Rule 10b-5(a) and (c) require scienter, while

negligence suffices for Section 17(a)(3). *Monarch Funding Corp.*, 192 F.3d at 308. Scheme liability “capture[s] a wide range of conduct.” *Lorenzo v. SEC*, 587 U.S. 71, 79 (2019).

Defendants can violate the scheme liability provisions by engaging in an “artful stratagem or a plan devised to defraud an investor.” *Id.* at 78 (cleaned up).

This Circuit has required something beyond making misstatements and omissions, such as dissemination, to find scheme liability under these provisions. *See SEC v. Rio Tinto*, 41 F.4th 47, 54-56 (2d. Cir. 2022). But Defendants are incorrect when they assert the additional conduct must be an “‘inherently deceptive act’ such as ‘sham agreements.’” Br. at 34. In *Lorenzo* itself, the Supreme Court upheld scheme liability for simply disseminating misstatements. In doing so, it made clear that “Congress intended to root out all manner of fraud in the securities industry. And it gave to the [SEC] the tools to accomplish that job.” *Lorenzo*, 587 U.S. at 85.

The Amended Complaint lists several instances in which Brown disseminated false and misleading statements made by SolarWinds (such as the Security Statement) and *vice versa*, as part of an overall scheme to conceal SolarWinds’ poor cybersecurity posture and increased cybersecurity risks. *See* AC ¶¶ 58, 61, 222-224. That scheme also included Brown’s misstatements, his misleading sub-certifications, and his efforts to construct, publish, and promote the false Security Statement. The scheme also included dissemination of some of the language that Defendants deride as puffery, which, even if not false and misleading by itself, was part of a campaign to make SolarWinds appear to be a cybersecurity leader, when in fact it was a laggard. *Compare id.* ¶ 222 (Brown claiming that SolarWinds “places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards”) *with id.* ¶ 228 (employee warning Brown that “we have a **systemic issue** around lack

of awareness for Security/ Compliance requirements with most if not all [of the information technology group's] projects.” (emphasis added))

Additionally, the Amended Complaint sufficiently alleges a coordinated effort where, with Senior InfoSec Manager E’s guidance, InfoSec Employee F falsely informed Palo Alto in November 2020 that SolarWinds had not previously seen similar activity from the Orion platform despite being aware of the USTP incident. *See id.* ¶ 283 (“Well, I just lied.”). This coordinated effort was made to avoid wider knowledge of SolarWinds’ cybersecurity problems and represented a separate set of acts apart from dissemination of the Security Statement in furtherance of the scheme. The Amended Complaint thus adequately pleads scheme liability.

D. The Amended Complaint Sufficiently Alleges Scienter.

1. Legal Standard for Scienter.

Scienter has been defined as “intent to deceive, manipulate, or defraud... or at least knowing misconduct.” *First Jersey*, 101 F.3d at 1467 (citations omitted). For violations of Section 17(a)(1) and Rule 10b-5, in addition to intentional conduct, “[i]t is well-settled that knowledge of the proscribed activity is sufficient scienter.” *SEC v. U.S. Envtl., Inc.*, 155 F.3d 107, 111 (2d. Cir. 1998) (collecting cases). Scienter can also be shown by recklessness, “which represents an extreme departure from the standards of ordinary care to the extent that the danger was either known to the defendant or so obvious that the defendant must have been aware of it.” *In re Carter-Wallace, Inc., Sec. Litig.*, 220 F.3d 36, 39 (2d Cir. 2000); *see also Novak*, 216 F.3d at 308-09 (defendants’ knowledge of or access to information contradicting public statements or failure to review information they had a duty to monitor show recklessness). Here, the Amended Complaint sets forth Brown’s knowledge regarding the misstatements and scheme conduct by showing that he sent or received copious information rendering the Security Statement and SEC filings misleading. *See, e.g.*, AC ¶¶ 83-88 (October 2018 NIST assessment with scores of “0” in

“Security Continuous Monitoring (Cloud),” “Detection Processes (Cloud),” and “Malicious code is detected (Cloud)”, and score of “1” in “Access permissions are managed, incorporating the principles of least privilege and separation of duties”), 89-91 (2019 NIST assessment with score of “1” in “Authentication, Authorization and Identity Management,” and score of “2” in Secure Software Development Lifecycle”), 192 (August 2019 presentation prepared by Brown stating that, “Access and privilege to critical systems/data is inappropriate.”). And the same facts also adequately allege Defendants’ negligence for purposes of Sections 17(a)(2) and (3). *See SEC v. Stoker*, 865 F. Supp. 2d 457, 468 n.12 (S.D.N.Y. 2012).

2. Brown Knew the Security Statement Was False.

Defendants argue that, even if the Amended Complaint sufficiently alleges that the Security Statement contained false or misleading statements related to SolarWinds’ cybersecurity practices, it does not allege scienter because SolarWinds and Brown were implementing a cybersecurity program throughout the Relevant Period that showed progress. *See Br.* at 40-43. Whether SolarWinds’ cybersecurity practices showed progress, however, does not bear upon whether Brown misrepresented the status of those practices. A person who knows there is a large hole in the bottom of a boat acts with scienter when saying the hull is sound, even if they are actively bailing the boat at the same time. Brown either knew, or was reckless in not knowing, of the Security Statement’s misrepresentations regarding SolarWinds’ NIST Cybersecurity Framework compliance, SDL policies, password policies, network monitoring, and access control policies. *See AC ¶¶ 10(a)-(l), 77, 79-88, 98-100, 119, 129, 152-153, 244.* Thus, Brown’s repeated approval of these false or misleading statements displays, at minimum, a “strong showing of reckless disregard for the truth.” *S. Cherry St*, 573 F.3d 98, 109 (2d Cir. 2009), *see also In re SolarWinds Corp.*, 595 F. Supp. 3d at 584 (“Plaintiffs sufficiently plead that Defendant Brown acted with, at least, severe recklessness when he touted the security measures

implemented at SolarWinds.”). As the chief cybersecurity officer and maker of the Security Statement, Brown’s scienter imputes to SolarWinds.

3. Brown Knowingly Provided False Information Related to the Risk Disclosures.

Defendants argue that, even if the risk disclosures were assumed to be materially false or misleading, the Amended Complaint does not allege scienter on the part of SolarWinds’ chief executive officer or chief financial officer. *See* Br. at 36-38. Contrary to Defendants’ argument, scienter for SolarWinds does not require scienter for the CEO or CFO. “When the defendant is a corporate entity...the pleaded facts must create a strong inference that someone whose intent could be imputed to the corporation acted with the requisite scienter.” *Teamsters Local 445 Freight Div. Pension Fund v. Dynex Cap. Inc.*, 531 F.3d 190, 195 (2d Cir. 2008); *see also Rex & Roberta Ling Living Trust v. B Commc’n Ltd.*, 346 F. Supp. 3d 389, 405-06 (S.D.N.Y. 2018); *Strougo v. Barclays PLC*, 105 F. Supp. 3d 330, 351-52 (S.D.N.Y. 2015).

Brown signed the sub-certifications relating to cybersecurity. *See* AC ¶¶ 298, 301. Those sub-certifications were relied on by the senior executives responsible for signing and certifying the SEC filings that contained the misleading disclosures. *Id.* Brown also provided information to the individuals who drafted these disclosures for SolarWinds. *Id.* ¶ 242. Brown intentionally or recklessly disregarded the numerous discrepancies between SolarWinds’ stated cybersecurity practices and the undisclosed deficiencies, as discussed above. *See id.* ¶¶ 299-301. As the principal officer at SolarWinds responsible for cybersecurity practices, Brown’s scienter should be imputed to SolarWinds. *See, e.g., Rex & Roberta Ling*, 346 F. Supp. 3d at 409 (“courts in this district have generally coalesced around the view that there is no requirement that the same individual who made an alleged misstatement on behalf of a corporation personally possessed the required scienter”) (cleaned up) (citing cases); *see also Loreley Fin. (Jersey) No. 3 Ltd. v.*

Wells Fargo Sec., LLC, 797 F.3d 160, 178 (2d Cir. 2015) (scienter can impute from “high-level” employees); *Kinross*, 957 F. Supp. 2d at 307 (scienter can impute from “senior management”).

Additionally, the widespread corporate failures alleged in the Amended Complaint support a finding that the SEC has pled scienter, or collective negligence, for SolarWinds because even if Brown did not act with scienter regarding the risk disclosures, the disclosed risks so grossly differed from SolarWinds’ actual risks that the Company must have deviated from the standards of ordinary care regarding them. *See Teamsters*, 531 F.3d at 195 (“it is possible to raise the required inference [of scienter] with regard to the corporate defendant without doing so with regard to a specific individual defendant”); *see also Bricklayers*, 866 F. Supp. 2d at 240 (“negligence is not a state of mind; it is a failure...to come up to the specified standard of care”).

4. Brown Was Tasked with Ensuring the December Form 8-K Was Technically Accurate, and Knew It Was Not.

Defendants argue that there was no scienter for the December 14, 2020 Form 8-K because SolarWinds promptly reported the SUNBURST attack after learning of it, and was still investigating the extent of the breach at the time. *See Br.* at 38-40. Brown participated in drafting the Form 8-K and was responsible for confirming the accuracy of the technical statements made in it. *Id.* ¶ 308. As discussed above, that Form 8-K misleadingly portrayed SUNBURST as merely something that “could potentially allow” an intrusion when Brown knew of three *actual* prior attacks over six months, including the USTP attack that had been described as “successful” and the Palo Alto attack that had been described as a “breach.” *See id.* ¶¶ 310-315.

The entire premise of Defendants’ argument is fallacious. A company can both act quickly to get ahead of bad news and downplay the bad news such that it knowingly or recklessly misleads the investing public. Nevertheless, Defendants argue that, even if the statements in the December 14, 2020 Form 8-K were inaccurate, there is no showing of scienter

because of the brief time between discovery of the SUNBURST attack and the Form 8-K and the fact that SolarWinds had hired an outside investigative firm whose work was incomplete. *See Br.* at 38-39. But Brown concluded at the time that no further work was necessary to connect the SUNBURST disclosure with the USTP and Palo Alto incidents. *See AC* ¶ 307. Thus, Brown’s decision not to disclose these events shows, at minimum, a “reckless disregard for the truth.” *S. Cherry St.*, 573 F.3d at 109. Furthermore, as the principal cybersecurity officer at SolarWinds, and given his authority over the technical accuracy of this statement, Brown’s scienter should be imputed to SolarWinds. *See Teamsters*, 531 F.3d at 195; *Rex and Roberta Ling Living Trust*, 346 F. Supp. 3d at 405-06, 409.

SolarWinds further argues that scienter is unsupported because it made a supplemental disclosure of the USTP and Palo Alto incidents in its January 12, 2021 Form 8-K, after it had conducted its investigation. *See Br.* at 39. Regardless of whether SolarWinds made the disclosure later, it still had an obligation to make an accurate disclosure of material facts at the time it made its December 14, 2020 Form 8-K. SolarWinds’ belated disclosure in the January 12, 2021 Form 8-K thus does not rescue its earlier, materially misleading statement.

5. Scienter for Scheme Liability Is Supported by Knowing or Reckless Dissemination of False Statements and Other Acts.

Defendants also argue that because SolarWinds had a security program, it is not true that a “policy was never followed.” *Br.* at 43. Again, this argument misconstrues the SEC’s allegations. The SEC’s scheme allegation is that Defendants engaged in a concerted course of business to deceive investors and customers regarding the quality of SolarWinds’ cybersecurity practices. This claim does not present a question of whether SolarWinds’ cybersecurity program existed. It asks whether Defendants knowingly or recklessly disseminated materially false information regarding SolarWinds’ cybersecurity practices. Brown’s continual efforts to falsely

promote SolarWinds' cybersecurity to investors and customers, right down to his "Brown Report" podcast, demonstrate his scienter with respect to this scheme. *See* AC ¶¶ 5, 56-64, 216.

III. The Amended Complaint Sufficiently Alleges Internal Accounting Controls Violations.

Exchange Act Section 13(b)(2)(B) requires, among other things, that issuers "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that...(iii) access to assets is permitted only in accordance with management's general or specific authorization." 15 U.S.C. § 78m(b)(2)(B)(iii). Section 13(b)(7) defines "reasonable assurances" as "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs." 15 U.S.C. § 78m(b)(7).

The Amended Complaint addresses at length how SolarWinds' insufficient cybersecurity controls failed to limit access to the Company's assets in accordance with management's authorization. *E.g.*, AC ¶¶ 323, 326; *see also id.* ¶¶ 76-77, 84-87, 90, 98-100. Among other things, SolarWinds' internal assessments rated its cybersecurity controls as deficient, including significant lapses around the company's access controls, its internal password policy, and the Secure Development Lifecycle for some of its products. *Id.* The Amended Complaint details at length a software engineer's warning of security gaps in the company's VPN access, through which an external attacker could (and eventually did) gain unauthorized access to SolarWinds source code, databases and products and use them in a larger attack that could damage SolarWinds financially and reputationally. *Id.* ¶¶ 10, 201-207, 209-210, 213. Those failures were documented in statements by Brown and others that "the current state of security leaves [SolarWinds] in a very vulnerable state for our critical assets" and that "[a]ccess and privilege to critical systems / data is inappropriate." *Id.* ¶¶ 1, 45, 48, 63, 241 ("current state of security"); ¶¶

10(e), 192 (“access and privilege”). The plain language of the statute and the allegations in the Amended Complaint demonstrate the sufficiency of the internal accounting controls claim.

A. Internal Accounting Controls Are Broader Than Controls Relating to Financial Reporting.

Seeking to avoid the plain language of the statute, Defendants and the Chamber of Commerce latch on to a single word in the statute, claiming that the word “accounting” limits the applicable controls only to those related to “financial reporting,” “the reliability of [issuers’] financial statements,” and “focus[ed]...on bookkeeping[.]” Br. at 47; Chamber Br. [ECF No. 68-1] at 2-4, 14, 19. This claim lacks merit. Since the passage of the Foreign Corrupt Practices Act of 1977 (“FCPA”), internal accounting controls have been recognized as being **broader** than simply controls relating to financial reporting, and specifically include controls relating to, among other things, safeguarding of assets. The SEC confirmed the breadth of the statutory provision when adopting related rules in 1979:

It bears emphasis that the accounting provisions of the FCPA are ***not exclusively concerned with the preparation of financial statements***. An equally important objective of the new law...is the goal of corporate accountability...Accordingly, new Section 13(b)(2) establishes requirements concerning the internal activities of reporting companies that are supportive of the disclosure system mandated by the Act, ***but should not be analyzed solely from that point of view***. The new requirements may provide an independent basis for enforcement action by the [SEC], whether or not violation of the provisions may lead, in a particular case, to the dissemination of materially false or misleading information to investors.

Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices, Rel. No. 34-15570 1979 WL 173674, at *6 (SEC Feb. 15, 1979) (emphasis added); *see also Statement of Management on Internal Accounting Control*, Rel. No. 34-16877, 1980 WL 20857, at *4 (SEC June 6, 1980) (reiterating that this provision is designed to codify “the obligation to provide shareholders with reasonable assurances that the business is adequately controlled”).

Before the enactment of the FCPA in 1977, Congress consulted the SEC and considered the American Institute of Certified Public Accountants (“AICPA”) Statement on Auditing Standards No. 1, § 320.28 (1973) (“SAS 1”) (Ney Decl. Ex. 6). Defendants and the Chamber of Commerce rely on this same standard. (Br. at 47-48; Chamber Br. at 2-3, 8-11). SAS 1 clarifies what is meant by an internal accounting control:

Accounting control comprises the plan of organization and the procedures and records that are concerned with safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that...[a]ccess to assets is permitted only in accordance with management’s authorization.

SAS 1, § 320.28 (emphasis in original).

As defined in SAS 1, “The objective of safeguarding assets requires that access to assets be limited to authorized personnel. In this context, access to assets includes both direct physical access and indirect access through the preparation and processing of documents.” SAS 1, § 320.42. Controls over the safeguarding of assets include limits on “[t]he number and caliber of personnel to whom access is authorized” and “[l]imitation of direct access to assets requir[ing] appropriate physical segregation and protective equipment or devices.” *Id.* The cybersecurity controls described in the Amended Complaint— access controls, limits on administrator rights and privileges, password protections, a Secure Development Lifecycle, and data loss prevention software to detect unauthorized access and actions—are precisely such internal accounting controls. *E.g.*, AC ¶¶ 178-179 (access controls and administrator rights and privileges), 160-161 (password protections), 110-113 (Secure Development Lifecycle), and 202-206 (data loss prevention software). Indeed, such controls are simply the digital-age equivalent of “physical segregation” and “protective equipment.” Defendants’ approach would exclude these provisions, and thus fundamentally depart from Congress’ intent in passing the statute.

B. Case Law Supports that Internal Controls Are Not Limited to Controls Related to Financial Statements.

Lacking support in the plain language and legislative history, Defendants and the Chamber of Commerce urge dismissal of the internal controls claim citing case law and legislative history but cite authorities involving *different* statutory provisions. First, they cite several cases enforcing different subsections of Section 13(b)(2)(B) and argue that these cases support dismissal, while failing to acknowledge that the decisions applying Section 13(b)(2)(B)(iii) instead support the SEC’s position. Br. at 48-49; Chamber Br. at 6-7, 11-15. Second, the Chamber of Commerce argues that the SEC’s guidance for a different phrase in the Sarbanes-Oxley Act of 2003 somehow alters the meaning of the term “internal accounting control” from the FCPA. Chamber Br. at 1-15. Both arguments lack merit.

All of the case law the SEC is aware of interpreting subsection (iii) of Section 13(b)(2)(B) aligns with the SEC’s position that controls concerning access to assets—regardless of any impact on financial reporting—constitute internal accounting controls. The court in *SEC v. Cavco Indus. Inc., et al.*, recently denied a defendant’s Motion to Dismiss the SEC’s Complaint alleging that the defendant violated the internal accounting controls provision, including the “access to assets” subsection. No. 2:21-cv-01507, 2022 WL 1491279, at *3 (D. Ariz. Jan. 25, 2022). The *Cavco* defendants relied on many of the same cases cited by the Defendants. *See* No. 2:21-cv-01507 (D. Ariz.), ECF No. 13 at 15. Still, the court rejected the argument that internal accounting controls were limited only to controls that directly impact the accuracy of a company’s financial reporting. Instead, it held that *Cavco*’s Insider Trading policies constituted an “internal accounting control” contemplated by Section 13(b)(2)(B)(iii). *Id.*

The only reported case known to the SEC that interprets the “access to assets” prong of Section 13(b)(2)(B) is *SEC v. World-Wide Coin Invs, Ltd.*, 567 F. Supp. 724 (N.D. Ga. 1983).

That court found that the company violated Section 13(b)(2)(B)(iii) by failing to adequately limit access to physical assets, *e.g.*, bullion and coins, to appropriate personnel. *Id.* at 752. This is analogous to SolarWinds’ failure to limit access to its crown jewel assets. *See* AC ¶¶ 322, 324, 326. The *World-Wide* court made clear that “[w]hile this [internal accounting control] requirement is supportive of accuracy and reliability in the auditor’s review and financial disclosure process, this provision should not be analyzed solely from that point of view.” 567 F. Supp. at 749-750. Instead, “[t]he internal controls provision is primarily designed to give statutory content to an aspect of management’s stewardship responsibility, that of providing shareholders with reasonable assurance that the business is adequately controlled.” *Id.* at 750. The court recognized that “[i]nternal accounting controls’ must be distinguished from the accounting system typically found at a company” and must include controls that “make it difficult for its assets to be misappropriated.” *Id.*

Defendants and the Chamber of Commerce cite *SEC v. Rio Tinto Ltd.*, No. 17-cv-7994 (AT), 2019 WL 1244933, at *19 (S.D.N.Y., Mar. 18, 2019), *SEC v. Patel*, No. 07-cv-39 (SM), 2009 WL 3151143, at *35 (D.N.H. Sept. 30, 2009), and *SEC v. Felton*, No. 20-cv-822 (G), 2021 WL 2376722, at * 12 (N.D. Tex. 2021). Br. at 48-49; Chamber Br. at 7. But none of those cases involve subsection (iii) of Section 13(b)(2)(B). Instead, they involve subsection (ii) relating to recording of transactions, and do not address “access to assets” at all.

In re Elan Corp. Sec. Litig., 543 F. Supp. 2d 187 (S.D.N.Y. 2008), is even further afield. *See* Chamber Br. at 6-7. That case involved reporting of adverse medical events to the FDA, and did not touch upon the access to assets or the financial reporting provisions of Section 13(b)(2)(B). 543 F. Supp. 2d. at 222-223. Defendants’ citation to a cherry-picked footnote within *In re: Ikon Office Solutions, Inc. Sec. Litig.*, 277 F.3d 658, 672 n. 14 (3d Cir. 2002) likewise fails

to support their position as *Ikon* analyzed the responsibilities and obligations of an independent auditor—not the broader set of internal accounting controls at issue here. Br. at 48.

C. The ICFR Provision of the Sarbanes-Oxley Act Is Not Synonymous with the Internal Accounting Controls of the FCPA.

The Chamber of Commerce inaccurately claims that prior SEC guidance shows that internal accounting controls are limited to financial reporting risks. It claims, without citation, that the SEC has interpreted the phrase internal accounting control from the FCPA “*in pari materia*” with the phrase “internal control over financial reporting” from the Sarbanes-Oxley Act. Chamber Br. at 11-12. This is incorrect. Indeed, the SEC has long said that internal accounting controls encompass a broader set of controls than the comparatively narrow ICFR provision of subsequently enacted Sarbanes-Oxley Act of 2002. *See* Rel. No. 34-16877, 1980 WL 20857, at *4 (stressing that the Exchange Act’s internal accounting control provision is “much broader than the integrity of financial statements”); *see also* Rel. No. 34-15570, 1979 WL 173674, at *5-7. Congress’ intent that ICFR and internal accounting controls should not be read synonymously is further shown by the fact that Congress did not amend the Exchange Act to revise or supplant Section 13(b)(2)(B) in 2002. Instead, it passed an entirely separate provision regarding ICFR. And unlike ICFR, which focuses on a system of controls designed to prevent **material** misstatements in the financial statements, Congress purposefully provided no materiality threshold for Section 13(b)(2)(B)’s requirement of internal accounting controls, which are broader by design and aimed at promoting good corporate governance. Thus, while the ICFR provision of the Sarbanes-Oxley Act is **consistent with** the financial reporting aspects of internal accounting controls, ICFR does not “subsume” the internal accounting controls concerning safeguarding of assets. Chamber Br. at 11.

For these same reasons, Defendants and the Chamber of Commerce’s citation to *In re Equifax*, 357 F. Supp. 3d at 1230, is unpersuasive. Br. at 49; Chamber Br. at 7. The *In re Equifax* court found that the plaintiffs failed to allege the falsity of a certification that Equifax maintained controls that would prevent misuse that would have a “material effect on the financial statements,” and in so doing relied extensively on the history of the Sarbanes-Oxley Act. 357 F. Supp. 3d at 1230-1231. As discussed, here the SEC has alleged violations of a different statute.

D. SolarWinds’ Products, Source Code, IT Infrastructure and Customer Databases Are Precisely the Types of “Assets” that SolarWinds’ Management Should Have Safeguarded.

Perhaps recognizing that history and case law are against their interpretation of Section 13(b)(2)(B), Defendants instead assert that SolarWinds’ products, source code and IT infrastructure are not “the sort of assets that would appear on [SolarWinds’] balance sheet.” Br. at 47. SolarWinds designs network monitoring software that it sells to customers. AC ¶ 43. SolarWinds’ Orion software platform that was compromised in the SUNBURST attack “accounted for 45% of its revenue in the first nine months of 2020.” *Id.* ¶¶ 3, 44, 285, 299. SolarWinds’ argument that those assets have “no nexus to accounting” is specious—it amounts to saying that the trucks manufactured by Ford, the parts used to manufacture those trucks, and the factories where those trucks are manufactured are not assets of the Ford Motor Company.⁷ Br. at

⁷ SolarWinds’ software development is capitalized and appeared on SolarWinds’ balance sheets. *See, e.g.*, Ney Decl. Ex. 3 SolarWinds’ 2020 Form 10-K at F-7, F-16, 46, 48 (addressing “Research and Development Costs”), F-25-28 (listing “developed product technologies” among intangible assets); Ex. 4 SolarWinds’ 2019 Form 10-K at F-6, F-16, 34, 38, 40, F-24-26 (same); Ex. 5 SolarWinds’ 2018 Form S-1/A Registration Statement, dated Oct. 18, 2018, at F-5-6, F-17-18, 58-59, 72, 74-75, 77, 80, 83-84, F-25-26, F-28 (same).

47. Both the accounting concept statement cited by the Chamber of Commerce⁸ and SolarWinds' own internal statements about the crown jewel Orion product support the claim that SolarWinds' products, source code, IT infrastructure, and customer databases are precisely the types of assets to which management must limit access. AC ¶¶ 44-45, 60, 187, 322.

IV. The Amended Complaint Sufficiently Alleges Disclosure Controls Violations.

The Amended Complaint sufficiently alleges that SolarWinds failed to maintain effective disclosure controls regarding potentially material cybersecurity risks and incidents.

A. Public Companies Must Maintain Effective Disclosure Controls.

Rule 13a-15(a) requires public companies to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer is accumulated and communicated to the management to allow for timely disclosure decisions. *See* 17 C.F.R. § 240.13a-15(a) and (e). Further, as the SEC has previously explained, disclosure controls and procedures “are intended to cover a broader range of information than is covered by an issuer’s internal controls related to financial reporting” and “should capture information that is relevant to an assessment of the need to disclose developments and risks that pertain to the issuer’s businesses.” *Certification of Disclosure in Companies’ Quarterly and Annual Reports*, Rel. No. 33-8124, 2002 WL 31720215, at *9, 67 Fed. Reg. 57276 (SEC Aug. 29, 2002).

Importantly, the mere existence of such policies is not in itself sufficient to satisfy the requirements of Rule 13a-15. Rather, Rule 13a-15 requires that an issuer’s policies be “effective”

⁸ The Financial Accounting Standards Board (FASB) Statement of Financial Accounting Concepts No. 8 (“SFAC 8”) (Ney Decl. Ex. 7), which was cited by the Chamber of Commerce, defines an asset as a “present right to an economic benefit...[which] entitles the entity to the economic benefit and the ability to restrict others’ access to the benefit.” SFAC 8 variously describes assets for accounting purposes as a thing that can “be exchanged for something else of value to the entity,” can be “used to produce something of value to the entity,” and “may be intangible...[and] useable by an entity in producing or distributing goods and services.” *See* Chamber Br. at 9, n. 5; SFAC 8, §§ E16-17, E19-20, E27-28, E33, E36.

at ensuring that management has the information it needs to make timely disclosure decisions. *See* 17 C.F.R. § 240.13a-15(b) (requiring an issuer’s management to evaluate on a regular basis “the effectiveness of the issuer’s disclosure controls and procedures”). Consequently, Defendants’ argument that Rule 13a-15(a) was not violated simply because SolarWinds had certain policies in place must fail. *See* Br. at 44. Maintaining effective disclosure controls requires more than just writing out a policy.

B. The Failure to Escalate Critical Information Shows that SolarWinds’ Controls Were Not Effectively Maintained.

During the Relevant Period, SolarWinds had an Incident Response Plan (“IRP”) that, in part, supposedly governed what information related to cybersecurity attacks should be escalated to the CEO and CTO for disclosure evaluation. AC ¶ 328. But no SolarWinds employees, including Brown, elevated certain material information about critical issues to executives responsible for disclosures. *See id.* ¶¶ 314-315, 328-330. Brown and others were either unaware of the requirements in the IRP or failed to recognize the applicability of the IRP’s notification requirement to the 2020 attacks and other red flags. *See id.* This failure to escalate information prevented the executives who were responsible for public disclosures from analyzing whether those issues warranted disclosure.

For example, SolarWinds’ IRP specified that a product security incident affecting more than one customer or affecting one customer but “for which other customers are susceptible” should be rated a level “2” / moderate incident and elevated to the CEO and CTO for disclosure evaluation. *Id.* ¶ 328. By rating both the USTP attack and Palo Alto attacks as “0” / minimal, crucial information was withheld from senior management’s disclosure analysis. The Defendants argue that this is “hindsight-biased second-guessing.” Br. at 45 n. 23. It is not. Rather, Defendants are again inappropriately attempting to argue facts on a motion to dismiss.

The SEC alleges that: (1) “Brown and others recognized that [Palo Alto] attack was linked to the [USTP] attack”; and that—in violation of the IRP—(2) “the attacks were still not reported to the CEO, nor was the CTO told about the [Palo Alto] attack.” AC ¶ 328. The SEC also alleges that Brown concluded at the time of the earlier USTP attack *either* “(1) the attacker was already at [USTP], or (2) someone was looking to use Orion in larger attacks” and that, after the Palo Alto attack, the first of those two options could almost certainly be excluded. *Id.* ¶ 286. Thus, based on Brown’s contemporaneous observations, these incidents should have triggered escalation pursuant to the IRP, no matter if, as Defendants contend, the ultimate “root cause of either incident” had not been determined. *Id.* ¶¶ 288, 328; Br. at 45 n. 23.

Additionally, linked attacks that indicate a compromise of a crown jewel asset are not “useless noise” (Br. at 45) but a scenario Brown described as “very concerning”—even before the second attack. AC ¶ 276. The failure, by Brown and others, to elevate these issues shows that SolarWinds failed to *maintain effective* disclosure controls.

C. Defendants’ View of Disclosure Controls Is Too Narrow.

Defendants offer an inappropriately narrow interpretation of Rule 13a-15. For example, Defendants argue that Brown’s failure to escalate the “VPN vulnerability” and customer incidents that Brown linked to SUNBURST are not relevant to a disclosure controls claim because those matters “were not required to be reported in the first place.” Br. at 43. Yet even if any particular critical security gap in isolation is not *required* to be *disclosed* to investors, that does not mean *per se* that their existence did not need to be *elevated* for disclosure *assessment*. This is especially true for issues relating to cybersecurity, which are particularly material to SolarWinds given its business model. *See* AC ¶ 103. And it is odd that SolarWinds claims that the USTP and Palo Alto attacks were not worthy of even being elevated for disclosure consideration, when they are matters that SolarWinds did eventually disclose.

D. Misstatements About Controls Are Not the Same Thing as Failing to Maintain Effective Controls.

Defendants also incorrectly attempt to shoehorn the disclosure controls claim into their own vision of a “repackaged omissions theory.” Br. at 43. But unlike private plaintiffs who are largely restricted to bringing fraud claims and must therefore allege misleading descriptions of controls, the SEC can bring a direct claim for violating Rule 13a-15, no matter how SolarWinds described their controls. Thus, the case law Defendants cite is completely distinguishable from this matter. For example, Defendants cite *Higginbotham v. Baxter Int’l, Inc.*, 495 F.3d 753, 760 (7th Cir. 2007), as “rejecting [a] controls claim where plaintiff failed to cite any different controls that should have been in place.” Br. at 46. But *Higginbotham* involved a court’s analysis of whether potentially inadequate controls raised an inference of scienter for a Rule 10b-5 fraud claim. 495 F.3d at 756. Likewise, *Arora v. HDFC Bank Ltd.*, involved an analysis as to whether statements related to the effectiveness of an entity’s internal controls supported a claim for securities fraud, and therefore does not advance Defendants’ theories. 671 F. Supp. 3d 305, 315 (E.D.N.Y. 2023) (“Conclusory allegations that a company made false or misleading statements that its controls were effective...absent specific allegations about how or why those controls were effective—do not state a claim for securities fraud.”). And, for the same reason, Defendants cannot avail themselves of the reasoning by this Court in *In re Hebron Tech. Co., Ltd. Sec. Litig.*, No. 20-cv-4420 (PAE), 2021 WL 4341500, at *20 (S.D.N.Y. Sept. 22, 2021) (dismissing securities fraud claims where plaintiff failed to plead a “sufficient basis on which to claim a false statement or material omission regarding the quality of company’s disclosure controls”).

V. The Amended Complaint Sufficiently Alleges Aiding and Abetting Liability.

The Amended Complaint pleads aiding and abetting liability for Brown for (1) the fraud claims under Rule 10b-5 and Section 17(a); (2) the false filing claims under Rules 13a-1, 13a-11,

13a-13, and 12b-20, [17 C.F.R. §§ 240. 13a-1, 13a-11, 13a-13, and 12b-20]; (3) the disclosure controls claim under Section 13(a) [15 U.S.C. § 78m]; and (4) the internal accounting controls claim under Section 13(b)(2)(B). Aiding and abetting requires knowingly or recklessly providing substantial assistance to a primary violation. *See* 15 U.S.C. § 78t(e) (aiding and abetting liability for persons who “knowingly or recklessly provides substantial assistance” to primary violation); *SEC v. Apuzzo*, 689 F.3d 204, 211, 211 n. 6 (2d Cir. 2012).

Defendants argue that the Amended Complaint does not adequately allege that Brown provided substantial assistance to statements or schemes that violate Rule 10b-5 or Section 17(a). *See* Br. at 49-50. As to the fraud claims, all of the SEC’s allegations and arguments supporting Brown’s primary liability for securities fraud also support that he aided and abetted SolarWinds’ fraud. *See Lorenzo*, 587 U.S. at 83 (“Those who disseminate false statements with intent to defraud are primarily liable under Rules 10b–5(a) and (c), § 10(b), and § 17(a)(1), even if they are secondarily liable under Rule 10b–5(b)”); *SEC v. Farnsworth*, No. 22-cv-8226 (KPF), --- F. Supp. 3d ---, 2023 WL 5977240, at *20 (S.D.N.Y. Sept. 14, 2023) (same factual allegations that supported scienter for defendant’s own statements supported aiding and abetting liability for co-defendant’s statements and show awareness of role in illegal scheme); *see also SEC v. Wilcox*, 663 F. Supp. 3d 146, 161 (D. Mass. 2023) (holding that pleading of primary violations with scienter also stated a claim for aiding and abetting liability) (citing *Lorenzo*).

For aiding and abetting SolarWinds’ false periodic SEC filings, the SEC also broadly relies on the allegations and arguments above but points the Court specifically to the allegations that Brown: (1) prepared and signed sub-certifications that SolarWinds relied on for the risk disclosures; and (2) provided information to those who drafted these disclosures for SolarWinds. AC ¶¶ 242, 298-301. For the false Form 8-K, the Amended Complaint sufficiently alleges that

Brown knowingly or recklessly aided and abetted that false filing when he told no one that he had already linked the prior attacks to the attack being disclosed and approved the technical accuracy of the Form 8-K that did not disclose those attacks. *See id.* ¶¶ 307, 314, 316.

Regarding the internal controls claim concerning SolarWinds’ cybersecurity practices, Brown was the principal officer at SolarWinds responsible for cybersecurity efforts, and by virtue of that position and his active role regarding these issues as described above and in the Amended Complaint, aided and abetted SolarWinds’ violation. *Id.* ¶¶ 236, 308, 314, 316.

As for disclosure controls, Brown’s failure to escalate issues and signing of sub-certifications, as discussed above, show that he knowingly provided substantial assistance. *See id.* ¶¶ 298, 301, 314-315, 328-330.

VI. Amici’s Policy Arguments Do Not Detract from the Sufficiency of the Allegations in the Amended Complaint.

Defendants and Amici⁹ advance multiple public-policy arguments, characterizing the SEC’s case as “unprecedented,” “completely out of the ordinary,” “novel,” and a “never before”-type case. But such depictions are simply not accurate. Indeed, this is not even the first lawsuit against these Defendants for these issues. The court in *In re SolarWinds Corp.*, a case premised on many of the same false statements, denied the Rule 12(b)(6) motion with respect to SolarWinds and Brown. 595 F. Supp. 3d at 587-88. Nor is it the first time that the SEC has brought cybersecurity-related charges. *See In the Matter of Altaba, Inc. f/d/b/a YAHOO!, Inc.*, Rel. No. 34-83096, 2018 WL 1919547 (SEC Apr. 24, 2018) (settled proceeding finding violations of antifraud and filing provisions of the securities laws where YAHOO! misleadingly described a cyber breach as possible when it knew one had already happened). Nor is it the first

⁹ Amici briefs are the Chamber Br., BSA/The Software Alliance (ECF 67)(“BSA Br.”), Chief Information Security Officers Amended Brief (ECF 96)(“CISO Br.”), and Former Government Officials (ECF 73)(“FGO Br.”).

time the SEC has charged a corporate officer who did not sign SEC filings with making false statements in other venues. *See, e.g., SEC v. Tolstedt*, 545 F. Supp. 3d 788, 794 (N.D. Cal. 2021) (fraud charges sufficiently alleged against Senior EVP of Community Banking at Wells Fargo for false and misleading statements about sales metric and signing false sub-certifications); *see also SEC v. Dragon*, 3:10-cv-1186 (S.D. Cal. June 2, 2010) (settled fraud case filed by SEC against senior vice president of research and development for making false statements to investors).

This is a disclosure case focused on SolarWinds' misleading public statements about its cybersecurity practices and risks. Amici try to carve out cybersecurity-related risks from statutory disclosure obligations regarding statements of material fact. But there is no such exception for cybersecurity. *See* SEC 2018 Cybersecurity Release, 2018 WL 993646, at *2 ("it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."). Put simply, cybersecurity-related or not, public companies cannot make material public misstatements about their internal controls. Defendants and Amici ask this Court for an exception, stating that acknowledging these material failures would make the company a target by threat actors. The securities laws do not permit this protection-by-deception approach. SolarWinds cannot make false statements about its cybersecurity to avoid being targeted by hackers any more than a bank can make false statements about its cash reserves to avoid a run on the bank.

Along with a novelty argument, Amici contend that the SEC is demanding: (a) "perfection" in cybersecurity; (b) disclosures of "roadmaps" that will benefit threat actors; and that (c) cybersecurity-related disclosures will have a "chilling" effect on open communication and internal cyber-related self-assessments. These arguments are addressed in turn.

A. The Securities Laws Do Not Require Perfect Cybersecurity, but They Do Require Accurate Disclosures.

Amici argue the SEC is requiring “perfectionism” in cybersecurity from public companies, and that “sanction[ing]” Defendants for one-single cyberattack would, among other horrors, “empower[] threat actors.” CISO Br. at 2-3, 13. But this is not a case about perfection, one-off failures, or the SEC imposing a specific, rigid system of controls. Rather, the SEC’s allegations focus on SolarWinds’ disclosures about practices that SolarWinds itself determined had failures, deficiencies, gaps, or problems. SolarWinds identified, internally, systemic failures that endured year, after year, after year, but misrepresented these failures to the investing public.

For example, despite publicly stating otherwise, during the Relevant Period SolarWinds failed to maintain a Secure Development Lifecycle, had poor access controls (including the rampant provisioning of administrative rights), had long-standing network monitoring failures, and failed to follow its stated password policy, among other findings. *See* AC ¶¶ 110-134 (Secure Development Lifecycle), 181-196 (access controls), 45 (employee training), 149-154 (network monitoring), 163-173 (password controls). Amici do little to address the misstatements in the Security Statement. When they do, Amici focus only on NIST, arguing that the SEC’s position that SolarWinds and Brown committed fraud for claiming to “follow” NIST “makes no sense.” CISO Br. at 10. They do not refute that the negative cybersecurity findings were extensive and went largely unaddressed. *See* AC ¶¶ 79-100 (detailing assessments conducted in 2017, 2018 and 2019 showing critical problems persisting organization-wide). The SEC is not alleging that any isolated incident in which a company fails to comply with its own cybersecurity controls is automatically a material incident that needs to be disclosed. Indeed, a single instance in which a non-compliant password is used is likely not material. But SolarWinds’ pervasive and sustained cybersecurity failures are a different matter entirely.

B. The Securities Laws Do Not Require Roadmaps, but They Do Require Accurate Disclosures.

Focusing largely on SolarWinds’ December 14, 2020 Form 8-K, Amici argue that incentivizing early detailed public disclosures of “vulnerability information” serves to “provide a roadmap to aid threat actors, and make companies less safe” by providing a “trove of useful intelligence” for threat actors. FGO Br. at 12; CISO Br. at 14; BSA Br. at 6-7. Contrary to Amici’s suggestion, “vulnerability information” is not the standard for disclosure. The SEC is not prescribing what SolarWinds should have said, roadmap or otherwise; SolarWinds just needed to include enough information to make its public statements not materially misleading.

The December 14, 2020 Form 8-K was materially misleading, because, among other things, it failed to disclose that the malicious code at issue had been actively exploited against SolarWinds’ customers multiple times over at least a six-month period. Far from providing a roadmap, this information was part of the total mix of information that would have been important to the investing public. By analogy, a bank that is robbed can disclose the material fact that robbers accessed its vault without also disclosing the exact details of how the robbers did so. Further, in its January 12, 2021 Form 8-K, SolarWinds did in fact relay to investors that two customers suffered attacks related to SUNBURST, which further undercuts Amici’s roadmap argument since SolarWinds itself later chose to disclose some of the information that the SEC alleges was missing from the earlier Form 8-K. (*See* Def. Ex. 4).

C. Required Disclosures Should Not Undermine Open Communication or Internal Assessments.

Amici argue that the SEC’s action will deter companies from creating a “‘trusted relationship’ with the Government,” and that they may chose not to share details of cyberattacks with the Government. CISO Br. at 23; FGO Br. at 10; BSA Br. at 5-9. Along the same lines, Amici argue that the SEC’s action will discourage collaboration on cybersecurity with other

companies, as well as internal reviews and self-assessments related to cybersecurity. CISO Br. at 17-20; BSA Br. at 10-15. As a preliminary matter, Amici make arguments based on facts outside the four corners of the Amended Complaint. The SEC alleges that, while participating in drafting the December 14, 2020 Form 8-K, Brown failed to convey—to anyone—his knowledge of the prior attacks at USTP and Palo Alto. AC ¶ 314. Brown testified he had immediately linked those attacks to SUNBURST with such certainty that any further analysis “wasn’t necessary.” AC ¶ 307. This is not a situation where there was considered discussion of whether to disclose something and a decision not to because it would harm a government investigation. This was Brown refusing to share his knowledge. Nonetheless, we will address Amici’s arguments in turn.

The SEC is tasked with ensuring that individuals who invest in public companies receive full and fair disclosures of the risks a company faces, and that information a company chooses to disclose is not materially misleading. Amici seem to suggest that complying with the law will have a chilling effect on the public-private partnership: that if companies are required to disclose material cybersecurity risks or attacks in a way that does not omit or mislead, they will somehow be deterred from disclosing them at all. But public companies are required to comply with many laws, regardless of the potential consequences and whether they are favorable to the company. Under periodic and episodic filings, issuers must disclose information that often includes adverse material information about earnings, revenue, and any material pending legal proceedings.¹⁰ Issuers still “work” with the government and still must comply with disclosure requirements.

Amici argue that the SEC’s case will chill cyber-related communications “among companies” who should be “helping other companies avoid the same problems.” BSA Br. at 14.

¹⁰ See, e.g., 17 C.F.R. §§ 229.303 (earnings and revenue); 229.103(a) (legal proceedings); 229.101(a)(1)(i) (business strategy); 229.101(a)(1)(iv) (acquisition or disposition of assets).

Again, relying on facts the four corners of the Amended Complaint, Amici embrace a view of peer company culture to which SolarWinds did not itself subscribe. For example, when Palo Alto reached out to SolarWinds in October 2020 about a malicious attack it experienced involving Orion, despite recognizing similarities to another recent attack, SolarWinds employees hid this fact and lied about the issue. *See* AC ¶ 283. Accordingly, the Court should not lend credence to an argument about supposed company peer culture that SolarWinds itself shirked.

Amici also suggest that there is a downside to disclosing corporate hygiene and material adverse events identified through internal company assessments—that such requirements undercut efforts to build “cyber resilience.” CISO Br. at 10. But the SEC has long asserted that “[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws.” SEC 2018 Cybersecurity Release, 2018 WL 993646, at *8. Such policies encourage companies to implement strong internal controls and robust reporting, which, among other results, help companies by assuring investors on these points, adequately valuing companies’ share price, and detecting and deterring fraud. Relatedly, and in SolarWinds’ case, internal security assessments are crucial to companies’ ability to obtain and retain business, and many vendors required SolarWinds to answer detailed security questionnaires. *See* AC ¶ 17. Thus, cybersecurity practices are information whose *accurate* disclosure is material.

CONCLUSION

For these reasons, the Court should deny Defendants’ motion to dismiss.

Respectfully submitted,

/s/ John J. Todor

John J. Todor

(admitted *pro hac vice*)

(signature block continues on next page)

Christopher M. Bruckmann
(SDNY Bar No. CB-7317)
Kristen M. Warden
(admitted *pro hac vice*)
William B. Ney
(admitted *pro hac vice*)
Benjamin Brutlag
(SDNY Bar No. BB-1196)
Lory Stone
(admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-5381 (Todor)
202-551-4661 (Warden)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
BruckmannC@sec.gov
TodorJ@sec.gov
WardenK@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

April 19, 2024

Attorneys for Plaintiff
Securities and Exchange Commission